Wireless Access Point 300
Wireless 802.11n con Switch 4 Porte 10/100

Manuale Utente
HNW300APN

www.hamletcom.com

SOMMARIO

Gentile Cliente,
La ringraziamo per la fiducia riposta nei nostri prodotti. La preghiamo di seguire le norme d'uso e manutenzione che seguono. Al termine del funzionamento di questo prodotto La preghiamo di non smaltirlo tra i rifiuti urbani misti, ma di effettuare per detti rifiuti una raccolta separata negli appositi raccoglitori di materiale elettrico/elettronico o di riportare il prodotto dal rivenditore che lo ritirerà gratuitamente.

Dichiarazione di responsabilità
L'importatore per l'Europa dichiara che il prodotto è conforme alle normative CE. I riferimenti all'importatore e le modalità di contatto sono disponibili su sito web www.hamletcom.com nella sezione CHI SIAMO del vostro paese.

L'importatore per L'Italia è:
Careca Italia S.p.A.
Partita IVA numero 02078660350
www.careca.com

Al fine di ridurre il materiale cartaceo a beneficio dell'ambiente riportiamo di seguito dichiarazione di conformità CE sintetica e guida rapida di installazione, rimandando al CD in allegato e al sito web tutta la documentazione estesa relativa al prodotto. Manuale utente in italiano ed eventuale manuale tecnico in inglese sono disponibili nel CD in allegato. La dichiarazione di conformità completa e tutta la documentazione relativa al prodotto è disponibile contattando direttamente il sito internet www.hamletcom.com all'indirizzo info@hamletcom.com specificando codice del prodotto e tipo documentazione richiesta.

Informiamo che il prodotto è stato realizzato con materiali e componenti in conformità a quanto previsto dalle direttive RoHS: 2002/95/CE, RAEE: 2003/96/CE, D.Lgs. 151/2005 e le direttive CE secondo i seguenti standard: ETSI EN 300 328 V1.7.1 (2006-10), ETSI EN 301-489-17: V1.3.2 (2008-04), ETSI EN 301-489-1: V1.8.1 (2008-04), IEC EN 60950-1: 2001 + A11: 2004, ETSI EN 300 386 V1.3.3 (2005-04).

CE Mark Warning
Questo dispositivo appartiene alla classe B. In un ambiente domestico il dispositivo può causare interferenze radio, in questo caso è opportuno prendere le adeguate contromisure.

Marchi commerciali
Tutti i marchi e i nomi di società citati in questa guida sono utilizzati al solo scopo descrittivo e appartengono ai rispettivi proprietari.

Variazioni
La presente guida ha scopo puramente informativo e può essere modificata senza preavviso. Sebbene questo documento sia stato compilato con la massima accuratezza, Hamlet non si assume alcuna responsabilità per eventuali errori od omissioni e all'uso delle informazioni in esso contenute. Hamlet si riserva il diritto di modificare o aggiornare il prodotto e la guida senza alcuna limitazione e senza obbligo di preavviso.

1. Introduzione

Hamlet HNW300APN è un Access Point Wireless a 300Mbit basato sullo standard IEEE 802.11n dotato di Switch 10/100 a 4 porte. E' la soluzione ideale per condividere un accesso ad Internet ad alta velocità anche senza fili. Le funzioni NAT e VPN di cui è dotato, consentono una ottima protezione da eventuali tentativi di intrusione da Internet, mentre la crittografia dei dati WEP e WPA garantisce analoga sicurezza nella comunicazione senza fili.

1.1 Requisiti di Sistema

- Processore Pentium 200MHZ o superiore
- Windows 98SE, Windows Me, Windows 2000, Windows XP, Windows Vista e Windows 7.
- 64MB di RAM o superiore.
- 25MB di spazio libero su disco

1.2 Contenuto della Scatola

- Wireless Access Point
- CD-ROM (Software & Manuale)
- Guida Rapida di Installazione
- Cavo Ethernet (RJ-45)
- Alimentatore

2. Specifiche

2.1 Significato dei LED

Sul lato anteriore del vostro Access Point sono presenti delle spie luminose. Consultate la seguente tabella per la spiegazione della funzione di ogni spia.

Power — Indicatore Alimentazione

WPS — Indicatore WPS Attivo

WAN — Indicatore WAN Attiva

1 — Indicatore Ethernet Attivo

WLAN — Indicatore Wireless Attivo

Icona	Colore	Acceso	Lampeggiante	Spento
Power	Verde	Pronto	In attesa che il dispositivo sia pronto	Access Point spento
WAN	Verde	Il dispositivo ha un indirizzo IP WAN dal Modem	Trasmette / Riceve Dati	Nessun indirizzo IP WAN dal Modem
WLAN	Verde	WLAN Pronta	Trasmette / Riceve Dati	WLAN Spenta
WPS	Verde	N/D	La connessione WPS si avvierà entro 2 minuti	WPS Inattivo
1	Verde	Ethernet Connessa	Trasmette / Riceve Dati	Ethernet Disconnesso

2.2 Connettori

La seguente tabella mostra le funzioni di ciascun connettore o switch del dispositivo.

CONNETTORE	DESCRIZIONE
ANTENNA	ANTENNA
ON/OFF SWITCH	Accende/Spegne il dispositivo
POWER	Si connette all'alimentatore in dotazione
LAN 4/3/2/1	Connette il dispositivo via Ethernet fino a quattro computer sulla tua LAN
WAN	Connette il dispositivo via Ethernet al Modem xDSL / Cable
WLAN	Premere questo tasto per almeno due secondi per attivare/disattivare i segnali wireless
WPS	Avvia la connessione WPS (Wi-Fi Protected Setup) entro due minuti

Figura 1. Vista posteriore dell'Access Point

Figura 2. Posizione dei pulsanti WLAN e WPS a lato dell'Access Point

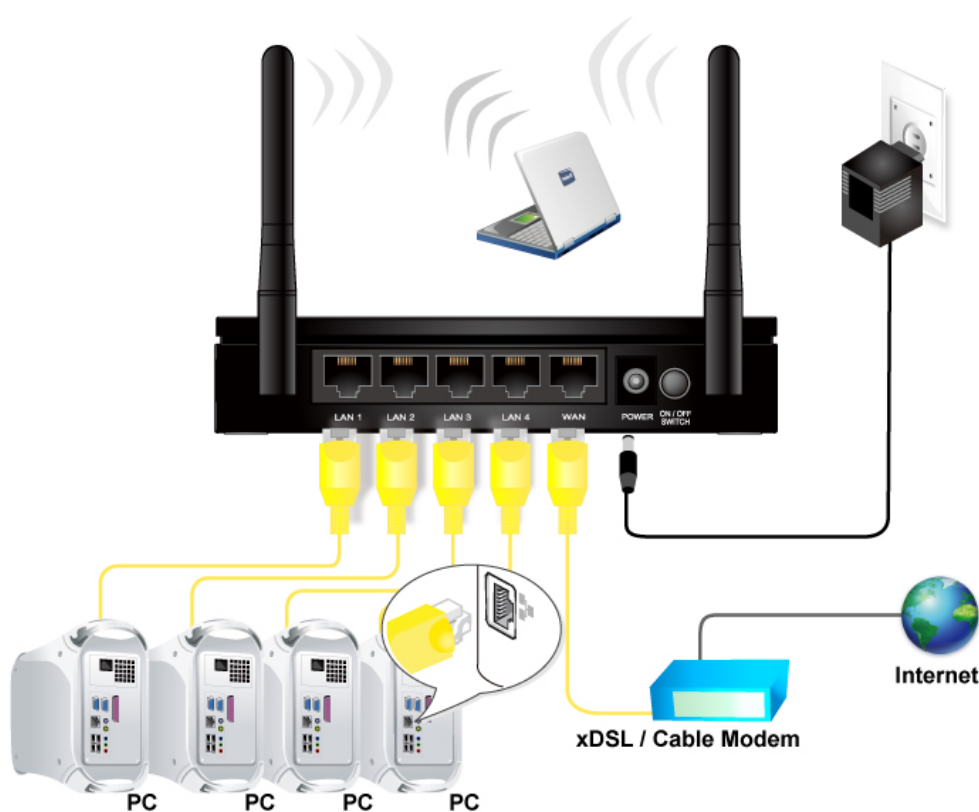
Figura 3. Posizione del pulsante di Reset (sotto all'Access Point)

3. Installazione & Configurazione

Seguite attentamente questi passi e passate al successivo solo dopo aver completato il passo precedente.

Nota: *Assicuratevi di essere ben isolati da ogni forma di alimentazione per evitare scariche elettriche*
Nota: *Usate solo l'alimentatore approvato dal costruttore e fornito con l'Access Point.*

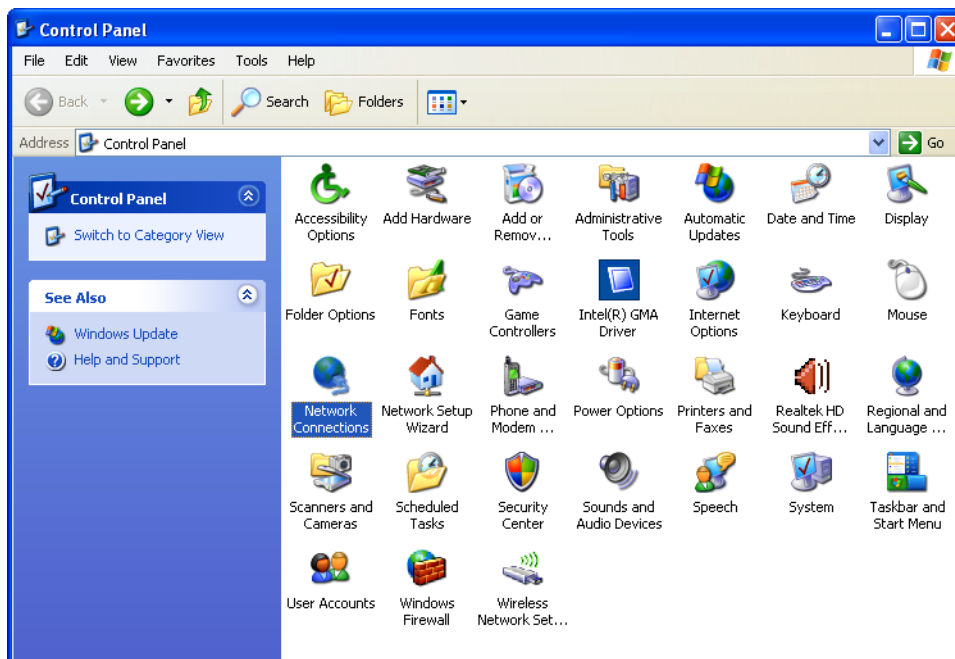
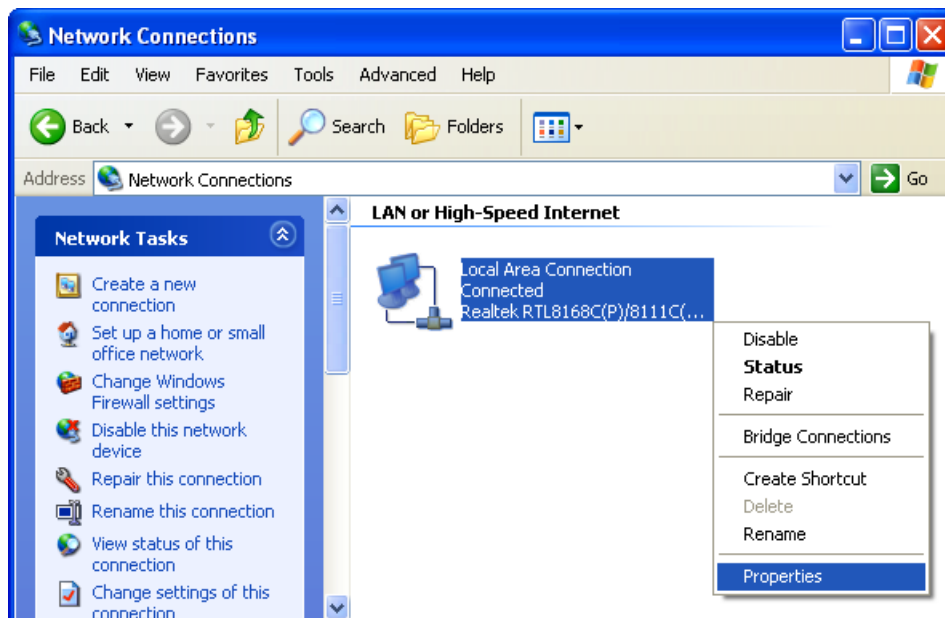
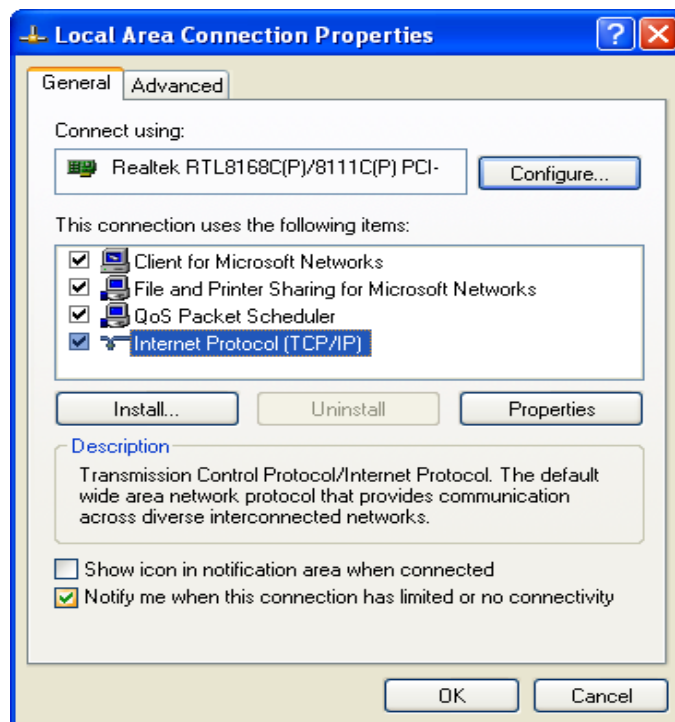
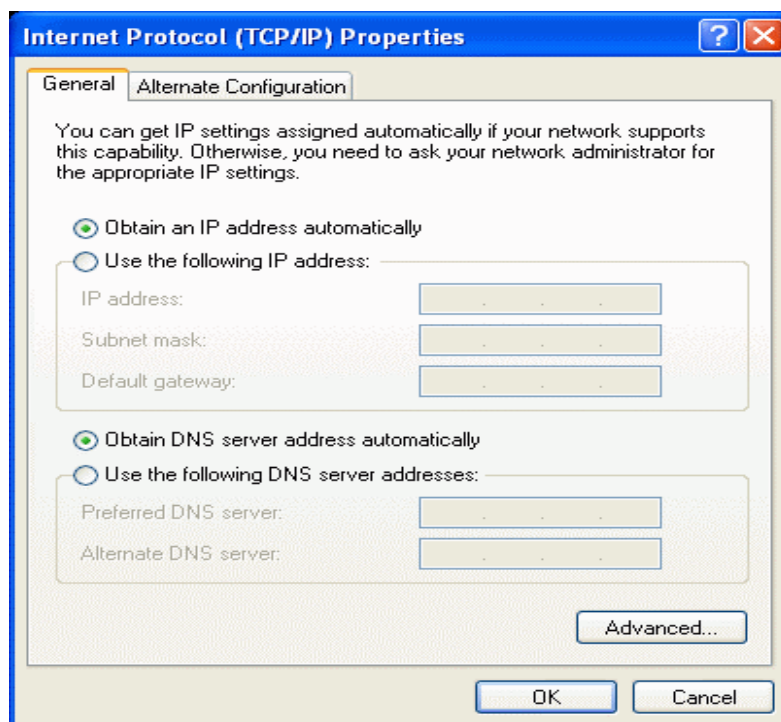
1. Collegate il cavo di alimentazione all'Access Point inserendo l'alimentatore nella presa elettrica.
2. Se il LED Power resta spento, consultate il capitolo "Risoluzione dei problemi" alla fine di questo manuale.

3.1 Collegamento dell'Access Point

1. Collegate il cavo Ethernet RJ45 in dotazione dalla porta Ethernet del vostro PC ad una delle 4 porte LAN dell'Access Point..
2. Collegate il cavo Ethernet RJ45 dalla porta Ethernet del vostro Modem ad una delle 4 porte LAN dell'Access Point.
3. Collegate l'adattatore alla presa di alimentazione "**Power**" dell'Access Point e accendete l'interruttore di alimentazione "**ON/OFF Switch**" del vostro Access Point.

4. Procedure di Configurazione

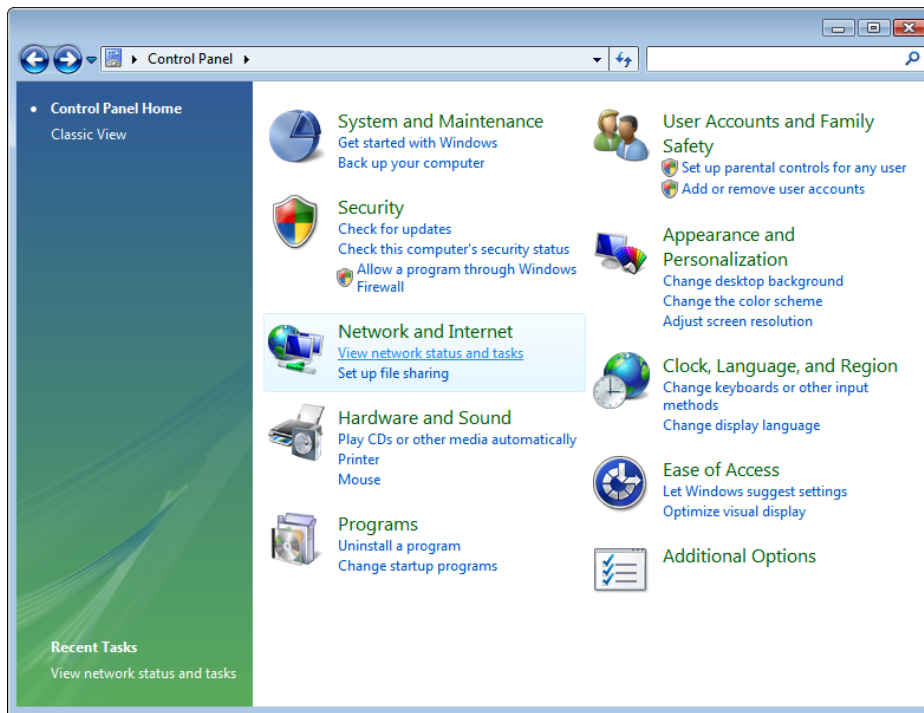
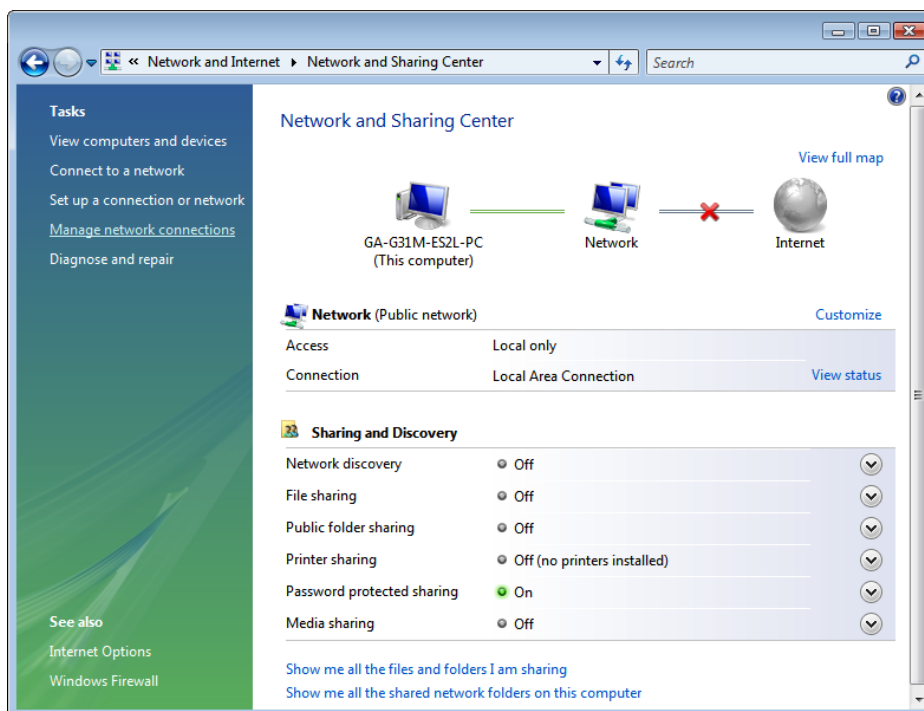
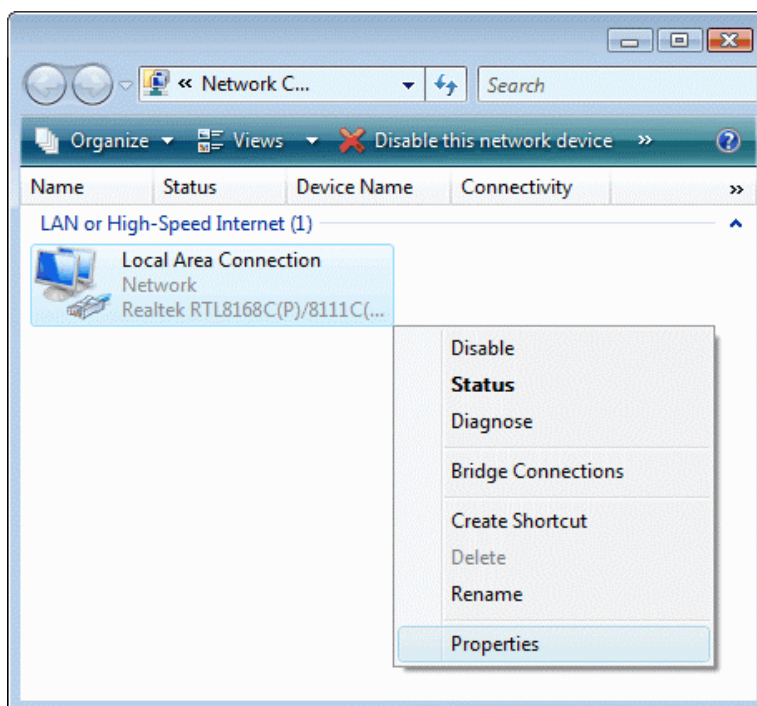
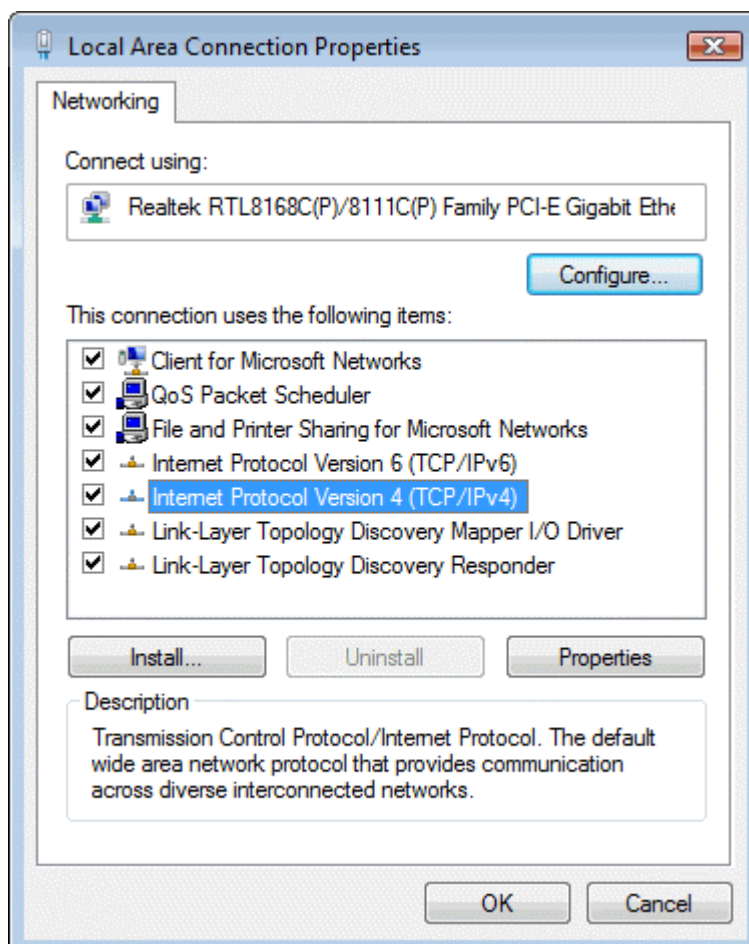
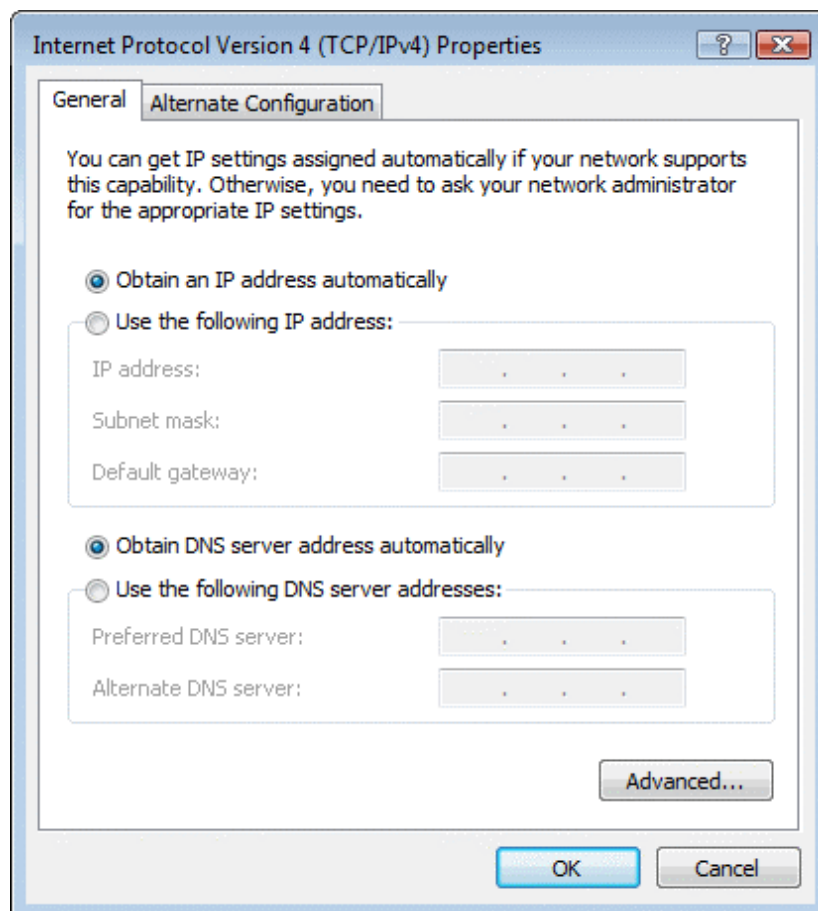
Prima di iniziare la configurazione dell'Access Point è necessario configurare il computer in modo che questo ottenga un indirizzo IP/DNS Server automaticamente.

4.1 Windows 98SE/ME/2000/XP

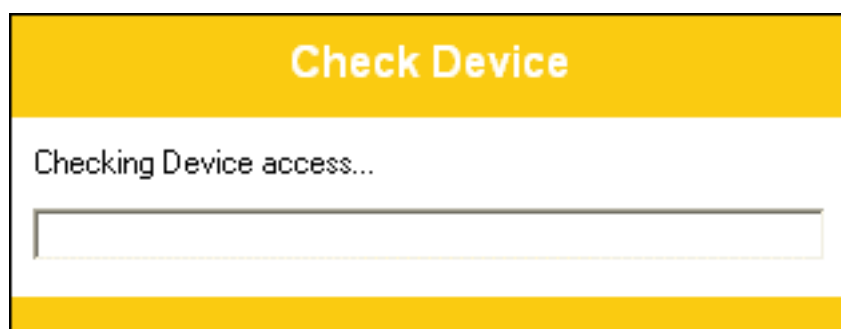
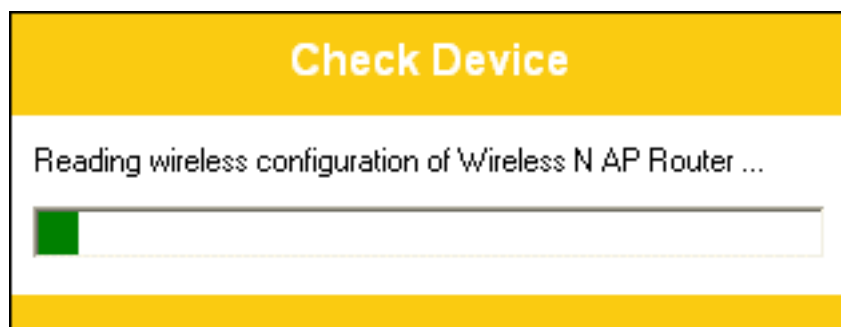
1. Cliccate su "**Start**" **>** "**Pannello di controllo**". Nel Pannello di Controllo, fate doppio click sull'icona "**Connessioni di rete**" per continuare.

2. Fate click con il tasto destro su "**Connessione alla rete locale**", quindi su "**Proprietà**.

3. Fate doppio click sulla voce “**Protocollo Internet (TCP/IP)** “.

4. Selezionate “**Ottieni automaticamente un indirizzo IP**” e “**Ottieni indirizzo server DNS automaticamente**” quindi cliccate su **OK** per continuare.

5. Cliccate su “**Mostra un’icona nell’area di notifica quando connesso**” (vedi immagine al punto 3) quindi cliccate su **OK** per salvare le impostazioni**.**

4.2 Windows Vista e 7

Le immagini mostrate nei passaggi seguenti si riferiscono a Windows Vista ma sono simili anche nel sistema operativo Windows 7

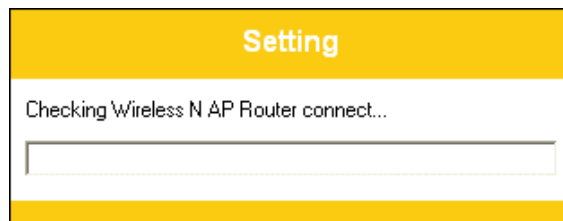
1. Fate click sul pulsante “**Start**” > “**Pannello di controllo**” > “**Centro connessioni di rete e condivisione**”.

2. Fate click su “**Gestisci connessioni di rete**” per continuare.

3. Fate click con il tasto destro su “**Connessione alla rete locale**“**,** quindi su “**Proprietà**”.

4. Fate doppio click sulla voce “**Protocollo Internet Versione 4 (TCP/IPv4).**)”.

5. Selezionate “**Ottieni automaticamente un indirizzo IP**” e “**Ottieni indirizzo server DNS automaticamente**” quindi cliccate su **OK** per continuare.

5. Configurazione dell'Access Point

1. Inserite il CD in dotazione nell'unità CD-ROM.
2. Il CD dovrebbe auto avviarsi, visualizzando la finestra mostrata di seguito. Se il CD non parte automaticamente, andate su Windows Explorer, selezionate l'unità del CD e fate doppio click su "**autorun.exe**.
3. Per configurare il dispositivo, cliccate su "**Configurazione Base**".

4. Il programma di configurazione sta controllando il dispositivo.

5. Il programma di configurazione sta controllando le impostazioni della wireless.

6. Selezionate la modalità di protocollo tra Fixed IP, DHCP client o PPPoE Mode ed inserite i relativi parametri forniti dal vostro ISP o dall'Amministratore della Rete e cliccate su "**Configurazione Wireless**".

7. Inserite l'"**ESSID**" se volete modificare le impostazioni predefinite (**Rete = Abilitata**, **ESSID = Hamlet**).
8. Se necessario, scegliete il tipo di Crittografia, come **Off – Nessuna Crittografia (Default)** / Crittografia a 64 Bit / Crittografia a 128 Bit / Accesso Protetto Wi-Fi (TKIP) / Accesso Protetto Wi-Fi 2 (AES-CCMP) e Modalità Mista di WPA. Ad esempio, potete scegliere la Modalità Mista di WPA e configurare la Password.
9. Cliccate su **"Submit"** per continuare.

10. Cliccate su “**Setup**” e quando la procedura sarà completata, verrà avviata la configurazione del dispositivo.

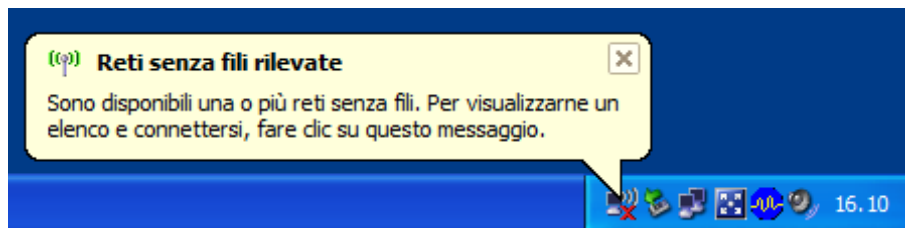
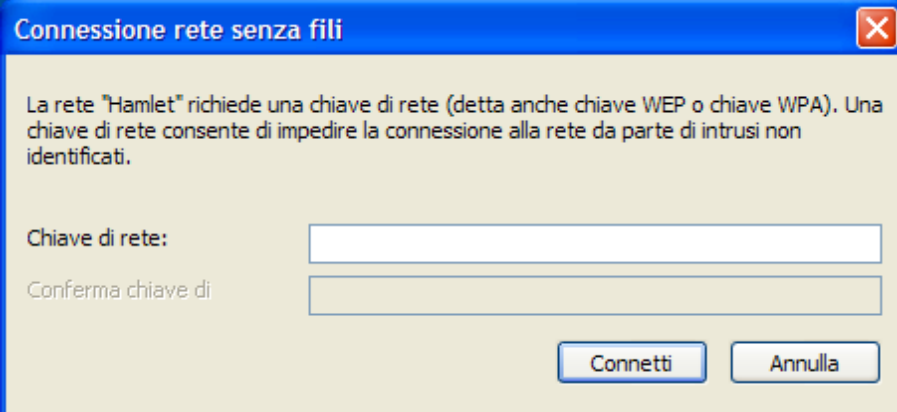
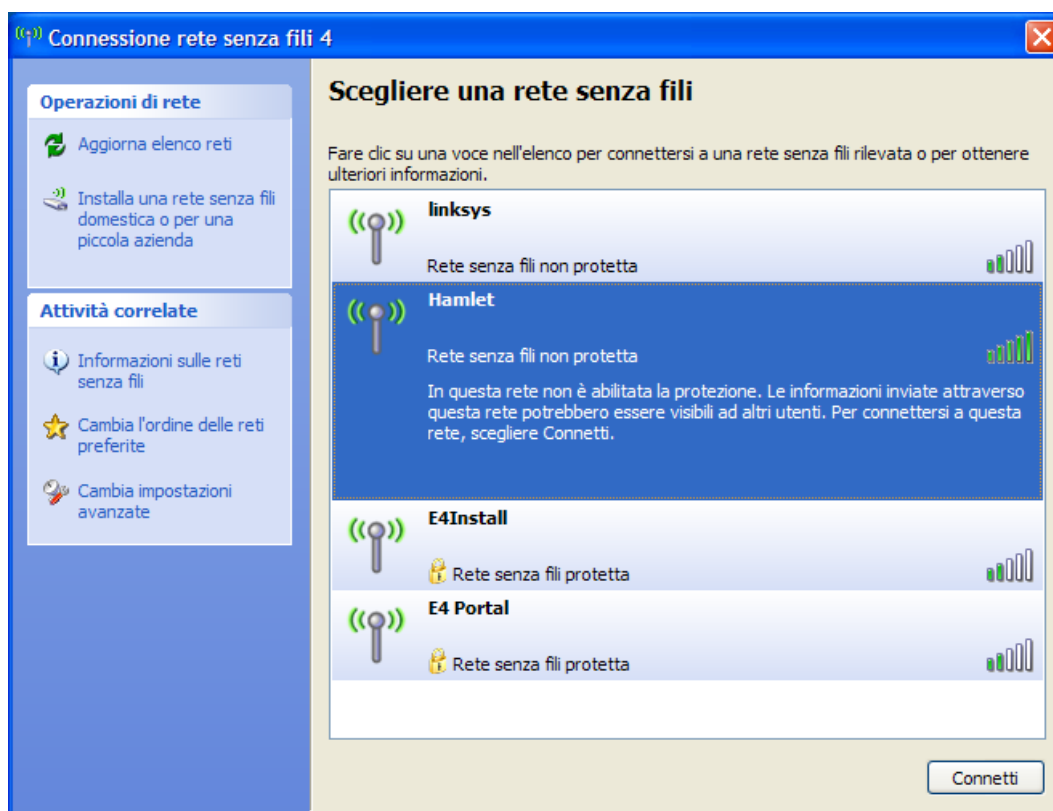
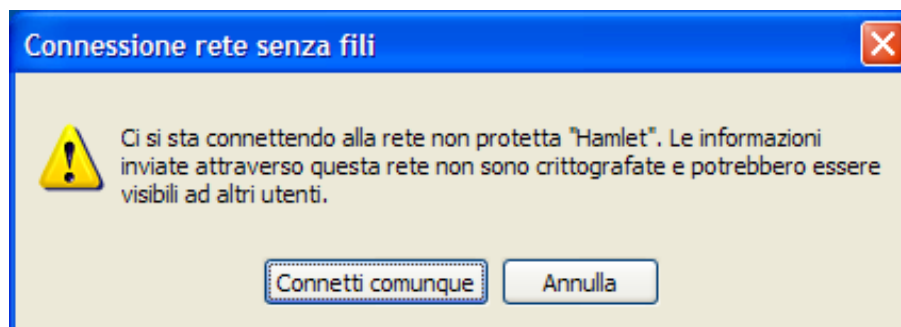
11. Vengono controllati l’hardware di connessione dell’Access Point, le impostazioni Internet, le impostazioni della WLAN e lo stato di connessione.

12. La configurazione delle impostazioni è completata. Cliccate su **"Close"** per uscire dal programma.

13. Cliccate ancora su "**Esci**" per uscire dal programma.

14. Ora l’Access Point è stato completamente configurato e pronto per connessioni Wireless ed Internet.

6. Creare una connessione Wireless

Ora che il programma di "Configurazione Base" è stato completato, è possibile connettersi al vostro Access Point Wireless. Seguire la procedura per creare una nuova connessione wireless.

1. Fate doppio click sull'icona della scheda wireless sul vostro computer e cercate la rete wireless per cui avete inserito il nome **"SSID"**.

2. Selezionate la rete wireless con il nome **"ESSID"** che avete scelto.

3. Se la rete wireless non è criptata, cliccate su **"Connetti comunque"** per connettervi.

4. Se la rete wireless è criptata, inserite la chiave di rete che appartiene alla modalità di Crittografia e la Password. Successivamente potrete modificare questa chiave di rete attraverso il menu di configurazione della rete wireless.

5. Cliccate su "**Connetti**" o su "**Applica**".

L'Access Point è ora configurato ed è pronto per connettersi ad Internet o alla vostra rete locale.

7. Configurazione Web

La configurazione web integrata permette di gestire l'Access Point da ogni postazione attraverso un browser come Internet Explorer o Firefox. Si consiglia di utilizzare una versione recente del browser con JavaScript abilitato.

7.1 Accedere all'interfaccia Web

1. Assicuratevi che l'Access Point sia correttamente collegato.
2. Predisponete il computer/rete di computer da connettere all'Access Point.
3. Lanciate il browser web e digitate "**http://192.168.1.254**" nella barra dell'indirizzo.
4. Verrà visualizzata la finestra di accesso in cui immettere il nome utente ("**admin**" è il nome preimpostato) e la password ("**hamlet**" è la password preimpostata) quindi cliccate su **OK**.
5. Ora dovrebbe apparire la pagina **Status** dell'Access Point.

Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:13h:32m:43s
Firmware Version	v1.4
Customer Version	REAN_v1.4_1T1R_STD_02_91229
Build Time	Tue Dec 29 19:16:36 CST 2009
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	11n_AP_Router
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:81:96:4f
Associated Clients	1
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
Default Gateway	10.0.0.2
DHCP Server	Enabled
MAC Address	00:13:33:81:96:4d
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.42
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
MAC Address	00:13:33:81:96:4e

8. Configurazione rapida

Attraverso la pagina "**Quick Setup**" potrete configurare l'Access Point in modo che si connetta ad Internet. Dal menu a sinistra fate click su *Quick Setup* e verrà visualizzata la seguente pagina:

Quick Setup

Operation Mode Setup

You can setup different modes to LAN and WLAN interface for NAT function.

◉ **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

○ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Next>>

8.1 Configurazione della Modalità Operativa

Potete impostare differenti modalità di interfaccia LAN e WLAN per la funzionalità NAT.

Gateway

In questa modalità, il dispositivo dovrebbe connettersi ad Internet attraverso Modem ADSL/Cavo. Il NAT è abilitato e i PC sulle quattro porte LAN condividono lo stesso IP attraverso la porta WAN. Il tipo di connessione può essere impostato nella pagina WAN tra PPPoE, client DHCP o IP statico.

Per cambiare la Modalità operativa:

1. Dal menu sulla sinistra, fate click su *Quick Setup*. Verrà visualizzata la seguente pagina:
2. Selezionate l'opzione *Gateway* quindi cliccate su *Next*>>.

Quick Setup

Operation Mode Setup

You can setup different modes to LAN and WLAN interface for NAT function.

◉ **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

○ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Next>>

ISP Wireless

In questa modalità, tutte le porte Ethernet sono collegate tra loro e il client wireless si connetterà all'Access Point dell'ISP. Il NAT è abilitato e i PC sulle porte Ethernet condividono lo stesso IP sulla rete LAN. Dovrete prima impostare la wireless in modalità client, quindi connettervi all'Access Point dell'ISP nella pagina Site-Survey. Il tipo di connessione può essere impostato nella pagina WAN tra PPPoE, client DHCP o IP statico.

Per cambiare la modalità operativa:

1. Dal menu sulla sinistra, fate click su *Quick Setup*. Verrà visualizzata la seguente pagina:
2. Selezionate l'opzione *Wireless ISP* quindi cliccate su *Next>>*.

Quick Setup

Operation Mode Setup

You can setup different modes to LAN and WLAN interface for NAT function.

○ **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

◉ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Next>>

8.2 Configurazione dell'Interfaccia WAN

Questa pagina è usata per configurare i parametri della rete Internet che si connette alla porta WAN del vostro Access Point. Qui potrete cambiare la modalità di accesso in IP statico, DHCP client, o PPPoE selezionandone la voce dal campo *WAN Access type*.

Per cambiare il tipo di accesso alla WAN:

1. Dal menu a tendina *WAN Access Type*, scegliete tra *Static IP, DHCP Client, PPPoE, PPTP, e L2TP* il valore definito dall'Amministratore della Rete o dall'ISP.
2. Cliccate su *Next>>*.

Quick Setup

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:

IP Statico

In questa modalità il dispositivo deve connettersi attraverso Modem ADSL/Cable. Il NAT è abilitato e i PC sulle quattro porte LAN condividono lo stesso IP attraverso la porta WAN.

1. Dal menu a tendina *WAN Access Type*, selezionate *Static IP*.
2. Inserite l'*IP Address*, ad esempio 172.1.1.1.
3. Inserite la *Subnet Mask*, ad esempio 255.255.255.0.
4. Inserite il *Default Gateway*, ad esempio 172.1.1.254.
5. Inserite il *DNS*, ad esempio 172.1.1.254.
6. Cliccate su *Next>>*.

Quick Setup

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:	Static IP
IP Address:	172.1.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	172.1.1.254
DNS :	172.1.1.254

Cancel <<Back Next>>

DHCP Client

1. Dal menu a tendina *WAN Access Type*, selezionate *DHCP Client*.
2. Cliccate su *Next>>*.

Quick Setup

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Cancel <<Back Next>>

PPPoE

1. Dal menu a tendina *WAN Access Type*, selezionate *PPPoE*.
2. Inserite la *User Name*, ad esempio 1234.
3. Inserite la *Password*, ad esempio 1234.
4. Cliccate su *Next>>*.

Quick Setup

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

8.3 Configurazione Base della Wireless

Questa pagina viene usata per configurare i parametri dei client della LAN wireless che si connettono al vostro Access Point.

Quick Setup

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band:	2.4 GHz (B+G+N)
Mode:	AP
Network Type:	Infrastructure
SSID:	11n_AP_Router
Channel Width:	40MHz
ControlSideband:	Upper
Channel Number:	11

Cancel <<Back Next>>

AP (Access Point)

AP viene usato per configurare i parametri dei client della LAN wireless che si connettono al vostro Access Point.

1. Dal menu a tendina *Band*, selezionate una banda.
2. Dal menu a tendina *Mode*, selezionate l'impostazione *AP*.
3. Inserite un *SSID*, ad esempio11n_AP_Router.
4. Dal menu a tendina *Channel Width*, selezionate un Channel Width.
5. Dal menu a tendina *ControlSideband*, selezionate un ControlSideband.
6. Dal menu a tendina *Channel Number*, selezionate un Channel Number.
7. Cliccate su *Next>>*.

Client

Questa pagina viene usata per configurare i parametri dei client della LAN wireless che si connettono al vostro Access Point.

1. Dal menu a tendina *Band*, selezionate una banda.
2. Dal menu a tendina *Mode*, selezionate l'impostazione *Client*.
3. Dal menu a tendina *Network Type*, selezionate un tipo di rete.
4. Inserite un *SSID*, ad esempio 11n_AP_Router.
8. Cliccate su *Next*>>.

WDS (Wireless Distribution System)

WDS è l'acronimo di Wireless Distribution System. Permette agli Access Point di essere connessi in modalità wireless. Un Dispositivo d'Accesso Integrato vi fornisce i servizi del WDS.

***Nota**: Il Dispositivo d'Accesso Integrato che supporta il WDS non supporta sistemi di sicurezza come WEP, WPA o WPA-Enterprise su una rete WDS:*

Potreste voler creare una rete multi-Access Point in casa o in ufficio, ma potreste non avere a disposizione un cablaggio Ethernet che raggiunga le postazioni degli altri Access Point.

Un modo per risolvere il problema è quello di usare un sistema realizzato in un Gateway Wireless e che è conosciuto come Wireless Distribution System (WDS).

Il WDS crea una rete a maglia fornendo un meccanismo che permetta agli Access Point di "parlare" tra loro, inviando dati ai dispositivi a loro associati.

***Nota:** Il WDS è basato su alcuni protocolli standard 802.11, ma non ci sono delle modalità standardizzate di implementazione. Quindi se avete un Gateway Wireless in una postazione e volete creare un collegamento WDS con un router di un'altra marca in un'altra postazione, probabilmente non funzioneranno.*

***Nota:** Quando usate il WDS come un sistema repeater, viene effettivamente dimezzata la velocità dei dati per i client connessi al Gateway Wireless integrato. Questo perché ogni bit dei dati deve essere inviato due volte (l'Access Point riceve e ritrasmette i dati).*

Per configurare il WDS, dovete modificare alcune impostazioni su ciascun Access Point della rete. Le procedure variano a seconda del marchio, ma in generale le procedure saranno simili alle seguenti:

Stazione WDS principale:

Una delle vostre stazioni WDS è quella principale per la rete WDS. Questo Access Point è direttamente collegato alla vostra connessione Internet, o collegato al vostro router attraverso una connessione cablata. La stazione principale fa da ponte alla vostra connessione Internet

Stazioni WDS Ripetitori:

In una semplice rete WDS composta di due Access Point, l'altro Access Point è un ripetitore. Questo riceve i dati dalla stazione principale e li ritrasmette ai client wireless associati e viceversa per i dati in arrivo dai client). Se avete più di due Access Point, gli Access Point remoti possono essere ripetitori o fungere da collegamenti che forniscono un punto di appoggio intermedio ai dati, nel caso in cui il ripetitore sia troppo lontano dalla stazione principale per comunicare.

Quando configurate la vostra stazione WDS principale, ricordate il canale che state impostando e l' ESSID o il nome della vostra rete. Nel caso il vostro Access Point abbia qualsiasi tipo di autoconfigurazione dei canali in grado di cambiare i canali in base alle condizioni della rete, assicuratevi che questa funzione sia disabilitata. Se la vostra stazione WDS è anche il vostro router, assicuratevi che sia impostato per distribuire gli indirizzi IP nella rete.

Nota: *Ricordate anche gli indirizzi MAC di tutte le vostre stazioni WDS in quanto molti programmi di configurazione richiedono che conosciate questi indirizzi per far funzionare le impostazioni della configurazione.*

Accendete nella vostra stazione principale la funzionalità WDS. A questo punto il programma di configurazione potrebbe chiedervi di identificare i ripetitori remoti.

In base al funzionamento del vostro software, potreste dover accedere separatamente al programma di configurazione sugli Access Point ripetitori remoti per accendere il WDS. Ricordate di:

1. Assegnare ogni altra stazione WDS allo stesso canale che sta usando la vostra stazione principale.
2. Impostare l'ESSID delle postazioni remote usando un nome unico o lo stesso nome che usate per la stazione principale.
3. Assicurarvi di non aver spento alcuna funzionalità di routing o DHCP nelle stazioni remote.

Solo WDS (Wireless Distribution System)

1. Dal menu a tendina *Band*, selezionate una banda.
2. Dal menu a tendina *Mode*, selezionate l'impostazione *WDS*.
3. Dal menu a tendina *Channel Width*, selezionate un Channel Width.
4. Dal menu a tendina *ControlSideband*, selezionate un ControlSideband.
5. Dal menu a tendina *Channel Number*, selezionate un Channel Number.
6. Cliccate su *Next>>*.

Quick Setup

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band:	2.4 GHz (B+G+N)
Mode:	WDS
Network Type:	Infrastructure
SSID:	11n_AP_Router
Channel Width:	40MHz
ControlSideband:	Upper
Channel Number:	11

Cancel <<Back Next>>

AP (Access Point) + WDS (Wireless Distribution System)

1. Dal menu a tendina *Band*, selezionate una banda.
2. Dal menu a tendina *Mode*, selezionate l'impostazione *AP+WDS*.
3. Inserite un *SSID,* ad esempio 11n_AP_Router.
4. Dal menu a tendina *Channel Width*, selezionate un Channel Width.
5. Dal menu a tendina *ControlSideband*, selezionate un ControlSideband.
6. Dal menu a tendina *Channel Number*, selezionate un Channel Number.
7. Cliccate su *Next*>>.

Quick Setup

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band: 2.4 GHz (B+G+N)

Mode: AP+WDS

Network Type: Infrastructure

SSID: 11n_AP_Router

Channel Width: 40MHz

ControlSideband: Upper

Channel Number: 11

Cancel <<Back Next>>

Solo MESH

1. Dal menu a tendina *Band*, selezionate una banda.
2. Dal menu a tendina *Mode*, selezionate l'impostazione *MESH*.
3. Dal menu a tendina *Channel Width*, selezionate un Channel Width.
4. Dal menu a tendina *ControlSideband*, selezionate un ControlSideband.
5. Dal menu a tendina *Channel Number*, selezionate un Channel Number.
6. Cliccate su *Next>>*.

Quick Setup

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band:	2.4 GHz (B+G+N)
Mode:	MESH
Network Type:	Infrastructure
SSID:	11n_AP_Router
Channel Width:	40MHz
ControlSideband:	Upper
Channel Number:	11

Cancel | <<Back | Next>>

AP (Access Point) + MESH

1. Dal menu a tendina *Band*, selezionate una banda.
2. Dal menu a tendina *Mode*, selezionate l'impostazione *AP+MESH*.
3. Inserite un *SSID,* ad esempio 11n_AP_Router.
4. Dal menu a tendina *Channel Width*, selezionate un Channel Width.
5. Dal menu a tendina *ControlSideband*, selezionate un ControlSideband.
6. Dal menu a tendina *Channel Number*, selezionate un Channel Number.
7. Cliccate su *Next*>>.

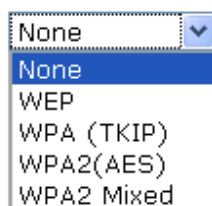
Quick Setup

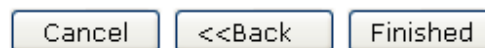
Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band:	2.4 GHz (B+G+N)
Mode:	AP+MESH
Network Type:	Infrastructure
SSID:	11n_AP_Router
Channel Width:	40MHz
ControlSideband:	Upper
Channel Number:	11

Cancel <<Back Next>>

8.4 Configurazione della Sicurezza della Wireless

Questa pagina vi permette di configurare le impostazioni della sicurezza della wireless. Accendete il WEP o la WPA e usando le Encryption Keys potrete prevenire ogni accesso non autorizzato alla vostra rete.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Potete proteggere i dati della wireless da potenziali *intercettatori* crittografando la trasmissione dei dati della wireless. Un intercettatore potrebbe configurare un adattatore wireless compatibile nel range del vostro dispositivo e cercare di accedere alla rete. Il crittografia dei dati ne consente il trasferimento in un formato non facilmente riconoscibile dagli utenti non autorizzati.

Ci sono due metodi di sicurezza della wireless tra cui scegliere:

- *Wired Equivalent Privacy (WEP)*; i dati vengono crittografati in blocchi di 64 o 128 bit, i quali possono solo essere inviati e ricevuti dagli utenti solo accedendo con una chiave di rete privata. Ogni PC nella vostra rete wireless deve essere configurato manualmente con la stessa chiave del vostro dispositivo per permettere la trasmissione dei dati. La WEP è considerata un'opzione di sicurezza di basso livello.
- *Wi-Fi Protected Access (WPA)*; garantisce una modalità più forte di crittografia dei dati (detta Temporal Key Integrity Protocol (TKIP)). Gira in una modalità speciale e semplice da configurare detta Pre-Shared Key (PSK) che permette di inserire manualmente una password su tutti i dispositivi della rete. La crittografia dei dati della WPA è basata su una chiave master della WPA, formata dalla password e dal nome della rete (SSID) del dispositivo.

Per configurare la sicurezza, scegliete una delle seguenti opzioni:

- Se non volete usare la sicurezza della rete wireless, dal menu a tendina *Encryption*, selezionate l'impostazione *None*, quindi cliccate su *Finished. None* è la configurazione preimpostata, ma è **fortemente raccomandato** di usare la sicurezza sul vostro dispositivo.
- Se volete usare la crittografia dei dati WEP 64bit ASCII (5 caratteri), seguite le istruzioni in *Configurare la crittografia 64bit ASCII (5 caratteri)*.
- Se volete usare la crittografia dei dati WEP 64bit Hex (10 caratteri), seguite le istruzioni in *Configurare la sicurezza WEP 64bit Hex (10 caratteri)*.
- Se volete usare la crittografia dei dati WEP 128bit ASCII (5 caratteri), seguite le istruzioni in *Configurare la sicurezza WEP 128bit ASCII (5 caratteri)*.
- Se volete usare la crittografia dei dati WEP 128bit Hex (10 caratteri), seguite le istruzioni in *Configurare la sicurezza WEP 128bit Hex (10 caratteri)*.
- Se volete usare la crittografia della password WPA1 - *Wi-Fi Protected Access 1 (TKIP)*, seguite le istruzioni in *Configurare la sicurezza della password WPA (TKIP)*.
- Se volete usare la crittografia WPA1 - *Wi-Fi Protected Access 1 (TKIP) HEX (64* caratteri*)*, seguite le istruzioni in *Configurare la sicurezza WPA (TKIP) HEX (64 caratteri)*.

- Se volete usare la crittografia della password WPA2 (AES) - *Wi-Fi Protected Access 2 (AES)*, seguite le istruzioni in *Configurare la sicurezza della password WPA2 (AES)*.
- Se volete usare la crittografia WPA2 (AES) - *Wi-Fi Protected Access 2 (AES) HEX (64* caratteri*)*, seguite le istruzioni in *Configurare la sicurezza WPA2 (AES) HEX (64 caratteri)*.
- Se volete usare la crittografia della password WPA2 Mixed- *Wi-Fi Protected Access 2 (Mista)*, seguite le istruzioni in *Configurare la sicurezza della password WPA2 (Mista)*.
- Se volete usare la crittografia WPA2 Mixed- *Wi-Fi Protected Access 2 (Mista) HEX (64* caratteri*)*, seguite le istruzioni in *Configurare la sicurezza WPA2 (Mista) HEX (64 caratteri)*.

Configurare la sicurezza WEP 64bit ASCII (5 caratteri)

L'esempio in questa sezione è della crittografia a 64bit.

1. Dal menu a tendina *Encryption*, selezionate l'impostazione *WEP*.
2. Dal menu a tendina *Key Length*, selezionate l'impostazione *64-bit*.
3. Dal menu a tendina *Key Format*, selezionate l'impostazione *ASCII (5 characters)*.
4. Digitate la chiave in *Key Setting*.
5. Cliccate su *Finished*.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption:	WEP
Key Length:	64-bit
Key Format:	ASCII (5 characters)
Key Setting:	*****

Cancel <<Back Finished

6. Modifiche effettuate con successo. Attendete durante il riavvio.

Change setting successfully!

Please wait for a moment while rebooting ...

Configurare la sicurezza WEP 64bit Hex (10 caratteri)

L’esempio in questa sezione è della crittografia a 64bit.

1. Dal menu a tendina *Encryption*, selezionate l’impostazione *WEP*.
2. Dal menu a tendina *Key Length*, selezionate l’impostazione *64-bit*.
3. Dal menu a tendina *Key Format*, selezionate l’impostazione *Hex (10 characters)*.
4. Digitate la chiave in *Key Setting*.
5. Cliccate su *Finished*.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WEP

Key Length: 64-bit

Key Format: Hex (10 characters)

Key Setting: **********

Cancel <<Back Finished

6. Modifiche effettuate con successo. Attendete durante il riavvio.

Change setting successfully!

Please wait for a moment while rebooting ...

Configurare la sicurezza WEP 128bit ASCII (13 caratteri)

L’esempio in questa sezione è della crittografia a 128bit.

1. Dal menu a tendina *Encryption*, selezionate l’impostazione *WEP*.
2. Dal menu a tendina *Key Length*, selezionate l’impostazione *128-bit*.
3. Dal menu a tendina *Key Format*, selezionate l’impostazione *ASCII (13 characters)*.
4. Digitate la chiave in *Key Setting*.
5. Cliccate su *Finished*.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WEP

Key Length: 128-bit

Key Format: ASCII (13 characters)

Key Setting: *************

Cancel <<Back Finished

6. Modifiche effettuate con successo. Attendete durante il riavvio.

Change setting successfully!

Please wait for a moment while rebooting ...

Configurare la sicurezza WEP 128bit Hex (26 caratteri)

L'esempio in questa sezione è della crittografia a 128bit.

1. Dal menu a tendina *Encryption*, selezionate l'impostazione *WEP*.
2. Dal menu a tendina *Key Length*, selezionate l'impostazione *128-bit*.
3. Dal menu a tendina *Key Format*, selezionate l'impostazione *Hex (26 characters)*.
4. Digitate la chiave in *Key Setting*.
5. Cliccate su *Finished*.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WEP

Key Length: 128-bit

Key Format: Hex (26 characters)

Key Setting: **************************

Cancel <<Back Finished

6. Modifiche effettuate con successo. Attendete durante il riavvio.

Change setting successfully!

Please wait for a moment while rebooting ...

Configurare la sicurezza della password WPA (TKIP)

L'esempio in questa sezione è della crittografia WPA (TKIP).

1. Dal menu a tendina *Encryption*, selezionate l'impostazione *WPA (TKIP)*.
2. Dal menu a tendina *Pre-Shared Key Format*, selezionate l'impostazione *Passphrase*.
3. Digitate la chiave in *Pre-Shared Key*.
4. Cliccate su *Finished*.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA (TKIP)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: 01234657

Cancel <<Back Finished

5. Modifiche effettuate con successo. Attendete durante il riavvio.

Change setting successfully!

Please wait for a moment while rebooting ...

Configurare la sicurezza WPA (TKIP) HEX (64 caratteri)

L'esempio in questa sezione è della crittografia WPA (TKIP) HEX (64 caratteri).

1. Dal menu a tendina *Encryption*, selezionate l'impostazione *WPA (TKIP)*.
2. Dal menu a tendina *Pre-Shared Key Format*, selezionate l'impostazione *HEX (64 characters)*.
3. Digitate la chiave in *Pre-Shared Key*.
4. Cliccate su *Finished*.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA (TKIP)

Pre-Shared Key Format: Hex (64 characters)

Pre-Shared Key: 01234657890123456789012345678

Cancel | <<Back | Finished

5. Modifiche effettuate con successo. Attendete durante il riavvio.

Change setting successfully!

Please wait for a moment while rebooting ...

Configurare la sicurezza della password WPA2 (AES)

L'esempio in questa sezione è della crittografia della password WPA2 (AES).

1. Dal menu a tendina *Encryption*, selezionate l'impostazione *WPA2 (AES)*.
2. Dal menu a tendina *Pre-Shared Key Format*, selezionate l'impostazione *Passphrase*.
3. Digitate la chiave in *Pre-Shared Key*.
4. Cliccate su *Finished*.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA2(AES)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: 01234657

Cancel <<Back Finished

5. Modifiche effettuate con successo. Attendete durante il riavvio.

Change setting successfully!

Please wait for a moment while rebooting ...

Configurare la sicurezza WPA2 (AES) HEX (64 caratteri)

L'esempio in questa sezione è della crittografia WPA2 (AES) HEX (64 caratteri).

1. Dal menu a tendina *Encryption*, selezionate l'impostazione *WPA2 (AES)*.
2. Dal menu a tendina *Pre-Shared Key Format*, selezionate l'impostazione *HEX (64 characters)*.
3. Digitate la chiave in *Pre-Shared Key*.
4. Cliccate su *Finished*.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA2(AES)

Pre-Shared Key Format: Hex (64 characters)

Pre-Shared Key: 012346578901234657890123465789

Cancel | <<Back | Finished

5. Modifiche effettuate con successo. Attendete durante il riavvio.

Change setting successfully!

Please wait for a moment while rebooting ...

Configurare la sicurezza della password WPA2 (Mista)

L’esempio in questa sezione è della crittografia della password WPA2 (Mista).

Questa crittografia supporta sia la WPA (TKIP) che la WPA2 (AES).

1. Dal menu a tendina *Encryption*, selezionate l’impostazione *WPA2 (Mixed)*.
2. Dal menu a tendina *Pre-Shared Key Format*, selezionate l’impostazione *Passphrase*.
3. Digitate la chiave in *Pre-Shared Key*.
4. Cliccate su *Finished*.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA2 Mixed

Pre-Shared Key Format: Passphrase

Pre-Shared Key: 01234657

Cancel <<Back Finished

5. Modifiche effettuate con successo. Attendete durante il riavvio.

Change setting successfully!

Please wait for a moment while rebooting ...

Configurare la sicurezza WPA2 (Mista) HEX (64 caratteri)

L’esempio in questa sezione è della crittografia WPA2 (Mista) HEX (64 caratteri).

Questa crittografia supporta sia la WPA (TKIP) che la WPA2 (AES).

1. Dal menu a tendina *Encryption*, selezionate l’impostazione *WPA2 (Mixed)*.
2. Dal menu a tendina *Pre-Shared Key Format*, selezionate l’impostazione *HEX (64 characters)*.
3. Digitate la chiave in *Pre-Shared Key*.
4. Cliccate su *Finished*.

Quick Setup

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA2 Mixed

Pre-Shared Key Format: Hex (64 characters)

Pre-Shared Key: 012346578901234657890123465789

Cancel <<Back Finished

5. Modifiche effettuate con successo. Attendete durante il riavvio.

Change setting successfully!

Please wait for a moment while rebooting ...

9. Modalità di funzionamento

Questo capitolo descrive come configurare la modalità con cui il vostro dispositivo si connette ad Internet. Esistono tre diverse modalità: Gateway, Bridge e ISP Wireless.

9.1 Configurazione della modalità di funzionamento

Per cambiare la modalità di funzionamento:

1. Dal menu sulla sinistra *Operation Mode* verrà visualizzata la seguente pagina:
2. Selezionate l'opzione *Gateway*, *Bridge* o *ISP Wireless* quindi cliccate su *Apply* per attivarla.

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

Gateway: In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.

Bridge: In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

Wireless ISP: In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.

Apply Change Reset

10. Rete Wireless

In questo capitolo si assume che abbiate già configurato i vostri PC wireless ed installato una scheda wireless compatibile sul vostro dispositivo. Vedete anche *Configurare PC wireless*.

10.1 Impostazioni di base

La pagina *Wireless Network* vi permette di configurare le proprietà wireless del vostro dispositivo. Per accedere alla pagina *Wireless Network Basic Settings*, dal menu *Wireless* sulla sinistra, cliccate su *Basic Settings*. Verrà visualizzata la seguente pagina:

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: AP Multiple AP

Network Type: Infrastructure

SSID: 11n_AP_Router

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

Associated Clients: Show Active Clients

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Apply Changes Reset

Campo	Descrizione
Disable Wireless LAN Interface	**Abilita/Disabilita l'Interfaccia della LAN Wireless.** **Default: Disabilitata**
Band	**Specifica la Modalità della WLAN: modalità mista 802.11b/g, modalità 802.11b o modalità 802.11g**
Mode	**Configura l'Interfaccia della LAN Wireless: modalità AP, Client, WDS, AP + WDS, MESH o AP + MESH**
Network Type	**Configura la tipologia di rete: Infrastructure o Ad hoc.**
SSID	**Specifica il nome della rete.** **Ciascuna rete LAN Wireless usa un nome di rete unico per identificare la rete. Questo nome è chiamato Service Set Identifier (SSID). Quando impostate il vostro adattatore wireless, specificate l'SSID. Se volete connettervi ad una rete esistente, dovete usare il nome di quella rete. Se state impostando una vostra propria rete, potete creare il vostro nome ed usarlo su ciascun computer. Il nome può essere composto al massimo da 20 caratteri e può contenere lettere e numeri.**
Channel Width	**Scegliere un Channel Width dal menu a tendina.**
Control Sideband	**Scegliere un Control Sideband dal menu a tendina.**
Channel Number	**Scegliere un Channel Number dal menu a tendina.**
Broadcast SSID	**Trasmette o nasconde l'SSID alla vostra rete.** **Default: Abilitata**
WMM	**Abilita/Disabilita il supporto Wi-Fi Multimedia (WMM).**
Data Rate	**Seleziona la velocità dei dati dal menu a tendina**
Associated Clients	**Mostra la tabella dei client wireless attivi** **Questa tabella mostra l'indirizzo MAC, la trasmissione, il contatore di ricezione dei pacchetti e lo stato di crittografia di ogni client wireless associato.**
Enable Mac Clone (Single Ethernet Client)	**Abilita Mac Clone (Single Ethernet Client)**
Enable Universal Repeater Mode	**Funziona come Access Point e come client contemporaneamente**
SSID of Extended Interface	**Quando la modalità è impostata su "AP" e URM (Universal Repeater Mode) è abilitato, l'utente deve inserire l'SSID di un altro AP nel campo "SSID of Extended Interface".**

10.2 Impostazioni avanzate

Queste impostazioni riguardano solo utenti con conoscenze tecniche avanzate sulle LAN wireless. Tali impostazioni non devono pertanto essere cambiate a meno che non conosciate gli effetti che eventuali modifiche avrebbero sul vostro Access Point. Per accedere alla pagina *Wireless Network Advanced Settings*, dal menu *Wireless* sulla sinistra, cliccate su *Advanced Settings*. Verrà visualizzata la seguente pagina:

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20-1024 ms)
Preamble Type: Long Preamble Short Preamble
IAPP: Enabled Disabled
Protection: Enabled Disabled
Aggregation: Enabled Disabled
Short GI: Enabled Disabled
WLAN Partition: Enabled Disabled
RF Output Power: 100% 70% 50% 35% 15%

Apply Changes Reset

Campo	Descrizione
Fragment Threshold	**Quando un pacchetto viene trasmesso sulla rete, a volte questo può essere rotto in diversi segmenti qualora le dimensioni fossero superiori a quelle permesse dalla rete.** **Il Fragmentation Threshold definisce il numero limite di byte usati.**
RTS Threshold	**RTS è l'acronimo di "Request to Send". Questo parametro controlla il limite delle dimensioni che un pacchetto può avere. Il valore preimpostato è 2347.**
Beacon Interval	**Inserire un valore beacon interval.**
Preamble Type	**Specifica se il Preamble type debba essere breve o lungo.**
IAPP	**Disabilita o abilita l'IAPP**
Protection	**Il meccanismo di protezione che previene collisioni tra nodi 802.11g.**
RF Output Power	**Misurazione TX Power.**

10.3 Sicurezza

Questa pagina vi permette di impostare la sicurezza della wireless. Accendete la WEP o la WPA attraverso l'Encryption Keys: potrete così prevenire l'accesso alla vostra rete wireless da parte di utenti non autorizzati. Per accedere alla pagina *Wireless Network Security*, dal menu *Wireless* sulla sinistra, cliccate su *Security*. Verrà visualizzata la seguente pagina:

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - 11n_AP_Router

Apply Changes Reset

Encryption: Disable

802.1x Authentication:

Campo	Descrizione
Select SSID	**Seleziona l'SSID**
Encryption	**Imposta la crittografia a Disabilitata, WEP, WPA , WPA2 o WPA-Mixed**
Use 802.1x Authentication	**Usa autenticazione 802.1x attraverso WEP 64bit o WEP 128bit**
Authentication	**Configura la modalità di autenticazione a Open System, Shared Key o Auto**
Key Length	**Imposta la lunghezza della chiave a 64-bit o 128-bit**
Key Format	**Imposta il formato della chiave ASCII (5 caratteri), Hex (10 caratteri), ASCII (13 caratteri) o Hex (26 caratteri)**
Encryption Key	**Permette di inserire l'Encryption Key**
WPA Authentication Mode	**Imposta la modalità di autenticazione WPA ad Azienda (RADIUS) o Personale (Pre-Shared Key)**
WPA Cipher Suite	**Imposta la WPA Cipher Suite a TKIP e/o AES**

Campo	Descrizione
WPA2 Cipher Suite	**Imposta la WPA2 Cipher Suite a TKIP e/o AES**
Pre-Shared Key Format	**Imposta il formato della Pre-Shared Key a Passphrase o HEX (64 caratteri)**
Pre-Shared Key	**Permette di inserire la Pre-Shared Key**
Enable Pre-Authentication	**Abilita/Disabilita il supporto di pre-autenticazione.** **Default: disabilitato.**
Authentication RADIUS Server	**Porta: Il numero della porta del Server RADIUS** **Indirizzo IP: l'indirizzo IP del Server RADIUS** **Password: la password del Server RADIUS**

WEP + Encryption Key

La WEP ha lo scopo di fornire sicurezza attraverso la crittografia dei dati su onde radio in modo da proteggerli quando vengono trasmessi da una postazione all'altra. Tuttavia oggi la WEP non è più ritenuta molto sicura:

1. Dal menu a tendina *Encryption*, selezionate l'impostazione *WEP*.
2. Dal menu a tendina *Key Length*, selezionate l'impostazione *64-bit* or *128-bit*.
3. Dal menu a tendina *Key Format*, selezionate l'impostazione *ASCII (5 characters), Hex (10 characters), ASCII (13 characters)* o *Hex (26 characters)*.
4. Inserite l'*Encryption Key* a seconda che abbiate selezionato ASCII o Hexadecimal.
5. Cliccate su *Apply Changes*.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - 11n_AP_Router

Apply Changes Reset

Encryption: WEP

802.1x Authentication:

Authentication: Open System Shared Key Auto

Key Length: 64-bit

Key Format: Hex (10 characters)

Encryption Key: **********

6. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

OK

WEP + Use 802.1x Authentication

1. Dal menu a tendina *Encryption*, selezionate l'impostazione *WEP*.
2. Selezionate l'opzione *Use 802.1x Authentication.*
3. Cliccate sul valore *WEP 64bits* o *WEP 128bits*.
4. Inserite *Port*, *IP Address* e *Password* del Server RADIUS:

Authentication RADIUS Server: Port 1812 IP address 192.168.1.1 Password ●●●●●●

5. Cliccate su *OK*.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

6. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

OK

WPA/WPA2/WPA2 Mixed + Personal (Pre-Shared Key)

Wi-Fi Protected Access (WPA e WPA2) è una classe di sistemi di sicurezza per le reti wireless (Wi-Fi) La WPA è progettata per lavorare con tutte le schede di rete wireless, ma non necessariamente con la prima generazione di Access Point wireless. La WPA2 implementa lo standard, ma non funziona con vecchie schede di rete. Entrambe garantiscono un buon livello di sicurezza, con due regole principali:

- La WPA o la WPA2 devono essere abilitate e preferite alla WEP.
- Nella modalità "Personal", la soluzione migliore per abitazioni e piccoli uffici, viene richiesta una password che dovrebbe essere più lunga delle solite password da 6 o 8 caratteri.

1. Dal menu a tendina *Encryption*, selezionate l'impostazione *WPA, WPA2* or *WPA2 Mixed*.

Encryption: WPA

Encryption: WPA2

Encryption: WPA2 Mixed

2. Selezionate l'opzione *Personal (Pre-Shared Key)*.

WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

3. Selezionate l'opzione *TKIP* e/o *AES* in *WPA Cipher Suite* se la vostra crittografia è la *WPA*:

WPA Cipher Suite: TKIP AES

4. Selezionate l'opzione *TKIP* e/o *AES* in *WPA2 Cipher Suite* se la vostra crittografia è la *WPA2*:

WPA2 Cipher Suite: TKIP AES

5. Selezionate l'opzione *TKIP* e/o *AES* in *WPA/WPA2 Cipher Suite* se la vostra crittografia è la *WPA2 Mixed*:

WPA Cipher Suite: TKIP AES

WPA2 Cipher Suite: TKIP AES

6. Dal menu a tendina *Pre-Shared Key Format*, selezionate l'impostazione *Passphrase* o *Hex (64 characters)*.

Pre-Shared Key Format: Passphrase

Pre-Shared Key Format: Hex (64 characters)

7. Inserite la *Pre-Shared Key* in base alla scelta di *Passphrase* o *Hex (64 characters)*.

Pre-Shared Key: 0123456789

8. Cliccate su *Apply Changes* per rendere effettive le modifiche.

Apply Changes

9. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

OK

WPA/WPA2/WPA2 Mixed + Enterprise (RADIUS)

Wi-Fi Protected Access (WPA e WPA2) è una classe di sistemi di sicurezza per le reti wireless (Wi-Fi) La WPA è progettata per lavorare con tutte le schede di rete wireless, ma non necessariamente con la prima generazione di Access Point Wireless. La WPA2 implementa lo standard, ma non funziona con vecchie schede di rete. Entrambe garantiscono un buon livello di sicurezza, con due regole principali:

- La WPA o la WPA2 devono essere abilitate e preferite alla WEP.
- Nella modalità "Personal", la soluzione migliore per abitazioni e piccoli uffici, viene richiesta una password che dovrebbe essere più lunga delle solite password da 6 o 8 caratteri.

1. Dal menu a tendina *Encryption*, selezionate l'impostazione *WPA, WPA2* or *WPA2 Mixed*.

2. Selezionate l'opzione *Enterprise (RADIUS)*.

WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

3. Selezionate l'opzione *TKIP* e/o *AES* in *WPA Cipher Suite* se la vostra crittografia è la *WPA*

WPA Cipher Suite: TKIP AES

4. Selezionate l'opzione *TKIP* e/o *AES* in *WPA2 Cipher Suite* se la vostra crittografia è la *WPA2*:

WPA2 Cipher Suite: TKIP AES

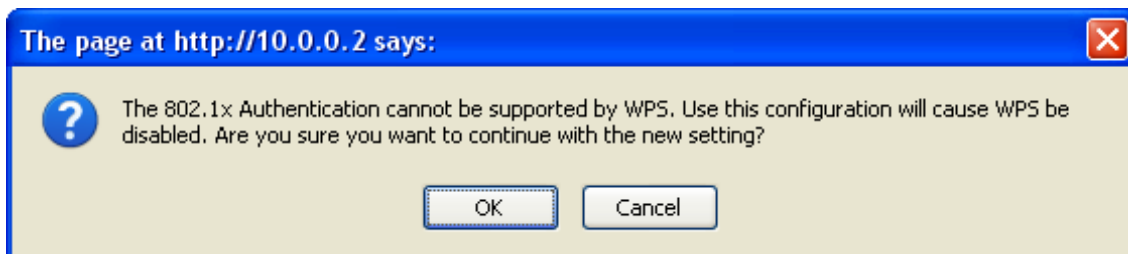
5. Selezionate l'opzione *TKIP* e/o *AES* in *WPA/WPA2 Cipher Suite* se la vostra crittografia è la *WPA2 Mixed*:

WPA Cipher Suite: TKIP AES

WPA2 Cipher Suite: TKIP AES

6. Inserite *Port*, *IP Address* e *Password* del Server RADIUS:

Authentication RADIUS Server: Port 1812 IP address 192.168.1.1 Password ••••••

7. Cliccate su *OK*.

8. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

OK

10.4 Access Control

Per ragioni di sicurezza, usando il MAC ACL (MAC Address Access List) si crea un ulteriore livello di difficoltà per poter attaccare la rete. Il MAC ACL viene creato e distribuito all'Access Point così che solo i NIC autorizzati possano connettersi alla rete. Questo può essere utilizzato insieme ad altre misure si sicurezza per aumentare il livello di complessità di intromissione nella rete.

Gli indirizzi MAC possono essere aggiunti/eliminati/modificati dalla lista ACL in relazione politica degli accessi MAC.

Se scegliete 'Allowed Listed', saranno in grado di connettersi al vostro Access Point solo i client i cui indirizzi MAC wireless sono nella lista di controllo degli accessi. Quando viene selezionato 'Deny Listed', questi client wireless nella lista non saranno in grado di connettersi all'Access Point. Per accedere alla pagina *Wireless Network Access Control*, fal menu *Wireless* sulla sinistra, cliccate su *Access Control*. Verrà visualizzata la seguente pagina:

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable

MAC Address: **Comment:**

Apply Changes Reset

Current Access Control List:

MAC Address	Comment	Select

Delete Selected Delete All Reset

Allow Listed

Se scegliete 'Allowed Listed', saranno in grado di connettersi al vostro Access Point solo i client i cui indirizzi MAC wireless sono nella lista di controllo degli accessi.

1. Dal menu a tendina *Wireless Access Control Mode*, selezionate l'impostazione *Allowed Listed*.
2. Inserite il *MAC Address*.
3. Inserite il *Comment*.
4. Cliccate su *Apply Changes*.

5. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

6. L'indirizzo MAC che avete creato è stato aggiunto al *Current Access Control List*.

Current Access Control List:

MAC Address	Comment	Select
00:11:22:33:44:55	Test1	☐

Delete Selected | Delete All | Reset

Deny Listed

Quando viene selezionato ‘Deny Listed’, questi client wireless nella lista non saranno in grado di connettersi all’Access Point.

1. Dal menu a tendina *Wireless Access Control Mode*, selezionate l’impostazione *Deny Listed*.
2. Inserite il *MAC Address*.
3. Inserite il *Comment*.
4. Cliccate su *Apply Changes*.

5. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

6. L’indirizzo MAC che avete creato è stato aggiunto al *Current Access Control List*.

Current Access Control List:

MAC Address	Comment	Select
00:11:22:33:44:55	Test1	☐

Delete Selected   Delete All   Reset

10.5 Impostazioni del WDS

Il Wireless Distribution System usa dei media wireless per comunicare con altri Access Point. Per far ciò, dovete impostare questi Access Point sullo stesso canale ed impostare l'indirizzo MAC degli altri Access Point con i quali intendete comunicare, quindi abilitare il WDS. Per accedere alla pagina *Wireless Network WDS settings*, dal menu *Wireless* sulla sinistra, cliccate su *WDS settings*. Verrà visualizzata la seguente pagina:

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

MAC Address:

Data Rate: Auto

Comment:

Apply Changes Reset Set Security Show Statistics

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select

Delete Selected Delete All Reset

Configurare solo il WDS (Wireless Distribution System)

1. Dal menu *Wireless*, cliccate su *Basic Settings*.
2. Dal menu a tendina *Mode*, selezionate l'impostazione *WDS.*
3. Dal menu a tendina *Channel Number*, selezionate un canale.
4. Cliccate su *Apply Changes*.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ **Disable Wireless LAN Interface**

Band:	2.4 GHz (B+G+N)	
Mode:	WDS	Multiple AP
Network Type:	Infrastructure	
SSID:	11n_AP_Router	
Channel Width:	40MHz	
Control Sideband:	Upper	
Channel Number:	11	
Broadcast SSID:	Enabled	
WMM:	Enabled	
Data Rate:	Auto	
Associated Clients:	Show Active Clients	

☐ **Enable Mac Clone (Single Ethernet Client)**

☐ **Enable Universal Repeater Mode (Acting as AP and client simultaneouly)**

SSID of Extended Interface:

Apply Changes Reset

7. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

8. Dal menu *Wireless*, cliccate su *WDS Settings*.
9. Selezionate l'opzione *Enable WDS*.
10. Inserite il *MAC Address*.
11. Inserite il *Comment*.

12. Cliccate su *Set Security*.

13. Questa pagina vi permette di configurare la sicurezza della wireless per il WDS. Quando è abilitato, dovete assicurarvi che ogni dispositivo WDS abbia adottato stessi algoritmo di crittografia e chiave.
14. Configurate ogni campo con l'*Encryption* che avete selezionato.
15. Cliccate su *Apply Changes*.

16. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

OK

17. Cliccate su *Close* per uscire dal *WDS Security Setup*.

18. Cliccate su *Apply Changes*.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☑ **Enable WDS**

MAC Address: 001122334455

Data Rate: Auto

Comment: Test1

Apply Changes | Reset | Set Security | Show Statistics

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select

Delete Selected | Delete All | Reset

19. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

OK

20. L'indirizzo MAC che avete creato è stato aggiunto al *Current Access Control List*.

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
00:11:22:33:44:55	Auto	Test1	☐

Delete Selected   Delete All   Reset

Configurare AP (Access Point) + WDS (Wireless Distribution System)

1. Dal menu *Wireless*, cliccate su *Basic Settings*.
2. Dal menu a tendina *Mode*, selezionate l'impostazione *AP+WDS.*
3. Inserite l'*SSID*, ad esempio 11n_AP_Router.
4. Dal menu a tendina *Channel Number*, selezionate un canale.
5. Cliccate su *Apply Changes*.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface
Band: 2.4 GHz (B+G+N)
Mode: AP+WDS Multiple AP
Network Type: Infrastructure
SSID: 11n_AP_Router
Channel Width: 40MHz
Control Sideband: Upper
Channel Number: 11
Broadcast SSID: Enabled
WMM: Enabled
Data Rate: Auto
Associated Clients: Show Active Clients
Enable Mac Clone (Single Ethernet Client)
Enable Universal Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Interface:
Apply Changes Reset

6. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!
OK

7. Dal menu *Wireless*, cliccate su *WDS settings*.
8. Selezionate l'opzione *Enable WDS*.
9. Inserite il *MAC Address*.
10. Inserite il *Comment*.
11. Cliccate su *Set Security*.

12. Questa pagina vi permette di configurare la sicurezza della wireless per il WDS. Quando è abilitato, dovete assicurarvi che ogni dispositivo WDS abbia adottato stessi algoritmo di crittografia e chiave.
13. Configurate ogni campo con l'*Encryption* che avete selezionato.
14. Cliccate su *Apply Changes*.

15. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

16. Cliccate su *Close* per uscire dal *WDS Security Setup*..

WDS Security Setup

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Encryption: None

WEP Key Format: ASCII (5 characters)

WEP Key:

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Apply Changes | Reset

17. Cliccate su *Apply Changes* button.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

MAC Address: 001122334455

Data Rate: Auto

Comment: Test1

Apply Changes | Reset | Set Security

Show Statistics

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select

Delete Selected | Delete All | Reset

18. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

21. L'indirizzo MAC che avete creato è stato aggiunto al *Current Access Control List*.

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
00:11:22:33:44:55	Auto	Test1	☐

Delete Selected | Delete All | Reset

10.6 Impostazioni Mesh

Una rete Mesh usa dei media wireless per comunicare con altri Access Point. Per far ciò, dovete impostare questi Access Point sullo stesso canale ed impostare lo stesso Mesh ID. Gli Access Point dovrebbero essere sotto la stessa modalità AP+MESH/MESH. Per accedere alla pagina *Wireless Mesh Network Setting*:, dal menu *Wireless* sulla sinistra, cliccate su *Mesh settings*. Verrà visualizzata la seguente pagina:

Wireless Mesh Network Setting

Mesh network uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel with the same Mesh ID. The APs should be under AP+MESH/MESH mode.

☐ **Enable Mesh**

Mesh ID: RTK-mesh

Encryption: None

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Apply Changes | Reset

Set Access Control | Show Advanced Information

Configurare solo impostazioni Mesh

1. Dal menu *Wireless*, cliccate su *Basic Settings*.
2. Dal menu a tendina *Mode*, selezionate l'impostazione *MESH.*
3. Dal menu a tendina *Channel Number*, selezionate un canale.
4. Cliccate su *Apply Changes*.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: MESH Multiple AP

Network Type: Infrastructure

SSID: 11n_AP_Router

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

Associated Clients: Show Active Clients

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Apply Changes Reset

5. Modifiche effettuate con successo. Cliccate su *Reboot Now* per rendere le modifiche effettive.

Change setting successfully!

Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.

Reboot Now Reboot Later

6. Dal menu *Wireless*, cliccate su *Mesh settings*.
7. Selezionate l'opzione *Enable Mesh*.

8. Inserite il *Mesh ID*.
9. Dal menu a tendina *Encryption*, selezionate un campo e configurate le relative voci.
10. Cliccate su Apply Changes.

Wireless Mesh Network Setting

Mesh network uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel with the same Mesh ID. The APs should be under AP+MESH/MESH mode.

11. Modifiche effettuate con successo. Cliccate su *Reboot Now* per rendere le modifiche effettive.

Change setting successfully!

Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.

Configurare AP (Access Point) + MESH

1. Dal menu *Wireless*, cliccate su *Basic Settings*.
2. Dal menu a tendina *Mode*, selezionate l'impostazione *AP+MESH.*
3. Inserite l'*SSID*, ad esempio 11n_AP_Router.
4. Dal menu a tendina *Channel Number*, selezionate un canale.
5. Cliccate su *Apply Changes*.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ **Disable Wireless LAN Interface**

Band: 2.4 GHz (B+G+N)

Mode: AP+MESH Multiple AP

Network Type: Infrastructure

SSID: 11n_AP_Router

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

Associated Clients: Show Active Clients

☐ **Enable Mac Clone (Single Ethernet Client)**

☐ **Enable Universal Repeater Mode (Acting as AP and client simultaneouly)**

SSID of Extended Interface:

Apply Changes Reset

6. Modifiche effettuate con successo. Cliccate su *Reboot Now* per rendere le modifiche effettive.

Change setting successfully!

Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.

Reboot Now Reboot Later

7. Dal menu *Wireless*, cliccate su *Mesh settings*.

8. Selezionate l'opzione *Enable Mesh*.
9. Inserite il *Mesh ID*.
10. Dal menu a tendina *Encryption*, selezionate un campo e configurate le relative voci.
11. Cliccate su Apply Changes.

Wireless Mesh Network Setting

Mesh network uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel with the same Mesh ID. The APs should be under AP+MESH/MESH mode.

12. Modifiche effettuate con successo. Cliccate su *Reboot Now* per rendere le modifiche effettive.

Change setting successfully!

Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.

Site Survey

Questa pagina fornisce uno strumento per rilevare le reti wireless. Se non viene trovato alcun Access Point o IBSS, potete scegliere di connettervi manualmente quando è abilitata la modalità client. Per accedere alla pagina *Wireless Network WDS settings*, dal menu *Wireless* sulla sinistra, cliccate su *Site Survey*. Verrà visualizzata la seguente pagina:

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

List of APs

SSID	BSSID	Channel	Type	Encrypt	Signal
None					

List of Mesh Points

Mesh ID	MAC Adddress	Channel	Select
None			

Configurare Wireless ISP + Wireless client + Site Survey

1. Dal menu *Operation Mode*, selezionate l'impostazione *Wireless ISP*.
2. Cliccate su *Apply Changes*.

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

○ **Gateway:**	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.
○ **Bridge:**	In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
◉ **Wireless ISP:**	In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.

Apply Change   Reset

3. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

4. Dal menu *Wireless*, cliccate su *Basic Settings*.
5. Dal menu a tendina *Mode*, seleziona l'impostazione *Client.*
6. Inserite l'*SSID* dell'Access Point al quale volete connettervi, ad esempio 11n_AP_Router. Se non lo conoscete, saltate questo passo.
7. Cliccate su *Apply Changes*.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: Client Multiple AP

Network Type: Infrastructure

SSID: 11n_AP_Router

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

Associated Clients: Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Apply Changes Reset

8. Modifiche effettuate con successo. Cliccate su *OK* per confermare.

Change setting successfully!

OK

9. Dal menu *Wireless*, cliccate su *Site Survey*.
10. Cliccate su *Refresh*.
11. Ora potete vedere gli Access Point che sono stati rilevati dal Gateway Wireless.
12. Selezionate l’SSID dell’Access Point al quale il Gateway Wireless deve connettersi.

13. Cliccate su *Connect*.

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

List of APs

SSID	BSSID	Channel	Type	Encrypt	Signal
RTL867x-ADSL	00:13:33:00:00:89	7 (B+G)	AP	no	22
1234	00:13:33:81:96:8e	11 (B+G+N)	AP	WPA2-PSK	20
-sparq	00:13:33:00:00:88	5 (B+G)	AP	no	6

List of Mesh Points

Mesh ID	MAC Adddress	Channel	Select
None			

14. Connessione avvenuta con successo. Cliccate su *OK* per confermare.

Connect successfully!

10.7 WPS

Questa pagina vi permette di cambiare le impostazioni per il WPS (Wi-Fi Protected Setup). Con questa funzione potete fare in modo che i client wireless sincronizzino automaticamente le proprie impostazioni e si connettano in un minuto all'Access Point. Per accedere alla pagina *Wireless Network WPS*, dal menu *Wireless*, cliccate su *WPS*. Verrà visualizzata la seguente pagina:

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

Disable WPS

WPS Status: Configured UnConfigured

Reset to UnConfigured

Self-PIN Number: 62828475

Push Button Configuration: Start PBC

Apply Changes Reset

Client PIN Number: Start PIN

Campo	Descrizione
Disable WPS	**Selezionate questa casella e cliccate su "Apply Changes" per disabilitare la Wi-Fi Protected Setup. LA WPS è abilitata per default.**
WPS Status	**Quando le impostazioni dell'Access Point sono quelle di fabbrica, è predisposto per aprire la sicurezza e lo stato non modificato. Verrà mostrato dal "WPS Status" –Se visualizza già "Configured", alcuni registrar come Vista WCN non configureranno l'Access Point. Quindi gli utenti dovranno andare alla pagina "Save/Reload Settings" e cliccare su "Reset" per reimpostare i valori predefiniti.**
Self-PIN Number	**"Self-PIN Number" è un PIN dell'Access Point. Qualora gli utenti volessero cambiarlo, possono cliccare su "Regenerate PIN" e quindi su "Apply Changes". Inoltre se gli utenti volessero creare il proprio PIN, possono immettere un PIN di quattro cifre e cliccare su "Apply Changes".**
Push Button Configuration	**Cliccate su questo tasto per invocare il metodo PBC del WPS. Viene usato solo quando l'Access Point funge da registrar.**
Apply Changes	**Cliccate su questo tasto per rendere effettive le modifiche apportate.**
Reset	**Reimposta le configurazioni di default.**
Client PIN Number	**Viene usato solo quando gli utenti vogliono che la propria stazione si unisca alla rete.**

Impostazioni del WPS

La funzione WPS (Wi-Fi Protected Setup) permette di stabilire con facilità una connessione tra il router e i client wireless. Ogni client wireless compatibile WPS può stabilire una connessione sicura con il router semplicemente premendo un tasto o immettendo un codice PIN.

AP mode

Per l'AP mode, il Gateway Wireless supporta tre profili: registrar, proxy, e client. Il Gateway Wireless effettua automaticamente degli switch al profilo più appropriato in base al profilo dell'altro dispositivo o in base ad una specifica configurazione.

Infrastructure-Client mode

Nella Infrastructure-Client mode, il Gateway Wireless supporta solo il profilo enrollee. Se l'utente clicca su "Start PIN", su "Start PBC", o preme il tasto fisico sul Gateway Wireless, avvierà la ricerca di WPS AP.

Pagina di Configurazione Avanzata della Wireless

Gli utenti devono assicurarsi che il file "Broadcast SSID" sia impostato su "Enabled", altrimenti potrebbe essere compromesso il corretto funzionamento della WPS.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: AP [Multiple AP]

Network Type: Infrastructure

SSID: 11n_AP_Router

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

Associated Clients: [Show Active Clients]

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

[Apply Changes] [Reset]

10.8 operazioni dell'AP - AP come enrollee

L'Access Point non viene configurato da alcun registrar. In questo caso gli utenti non devono effettuare alcuna operazione lato Access Point ed hanno bisogno solo di inserire il codice PIN del dispositivo nel registrar. Viene di seguito fornito un esempio preso da Vista WCN:

1. Dal menu *Wireless* -> *WPS* verrà visualizzata la seguente pagina:
2. Assicuratevi che l'Access Point sia nello stato *UnConfigured*.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

Disable WPS

WPS Status: Configured UnConfigured

Reset to UnConfigured

Self-PIN Number: 26709543

Push Button Configuration: Start PBC

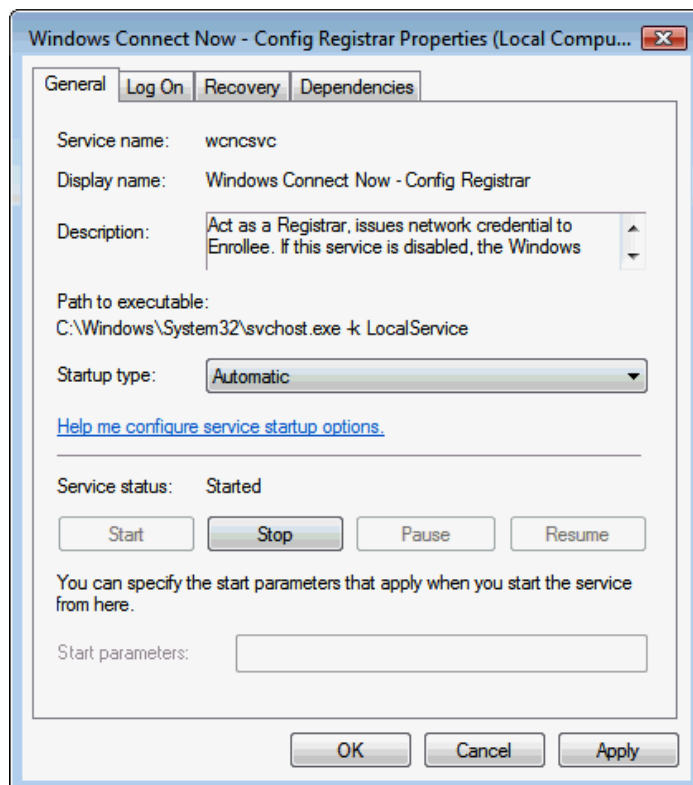
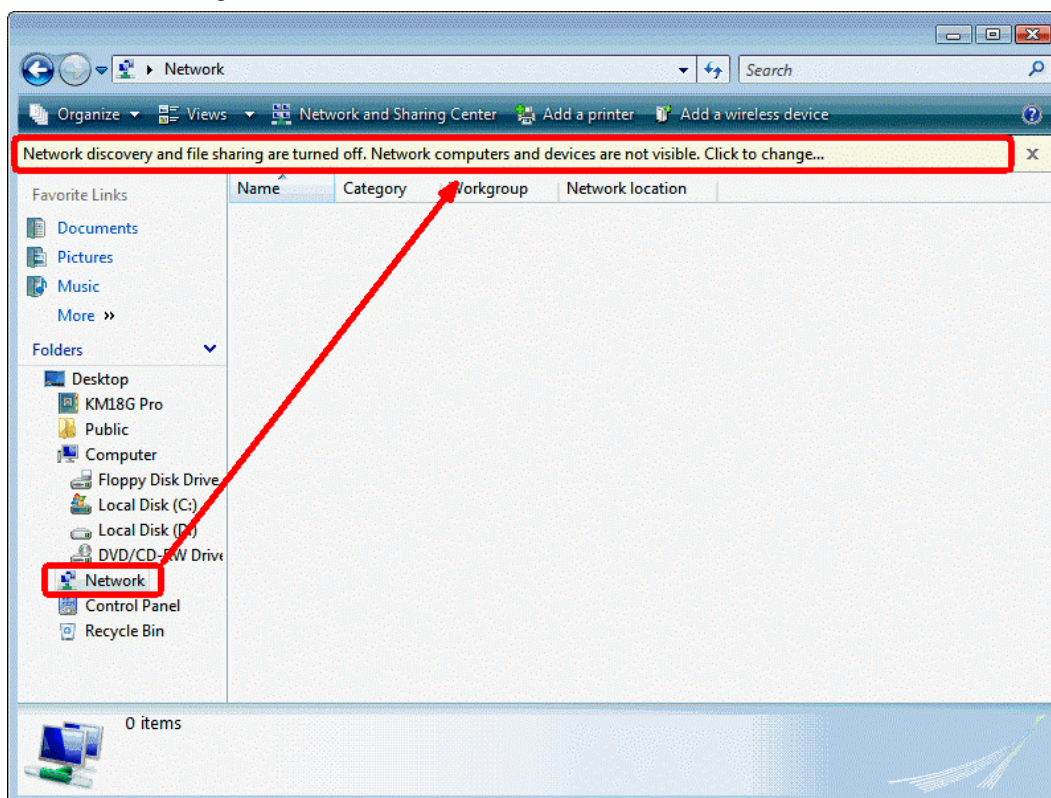
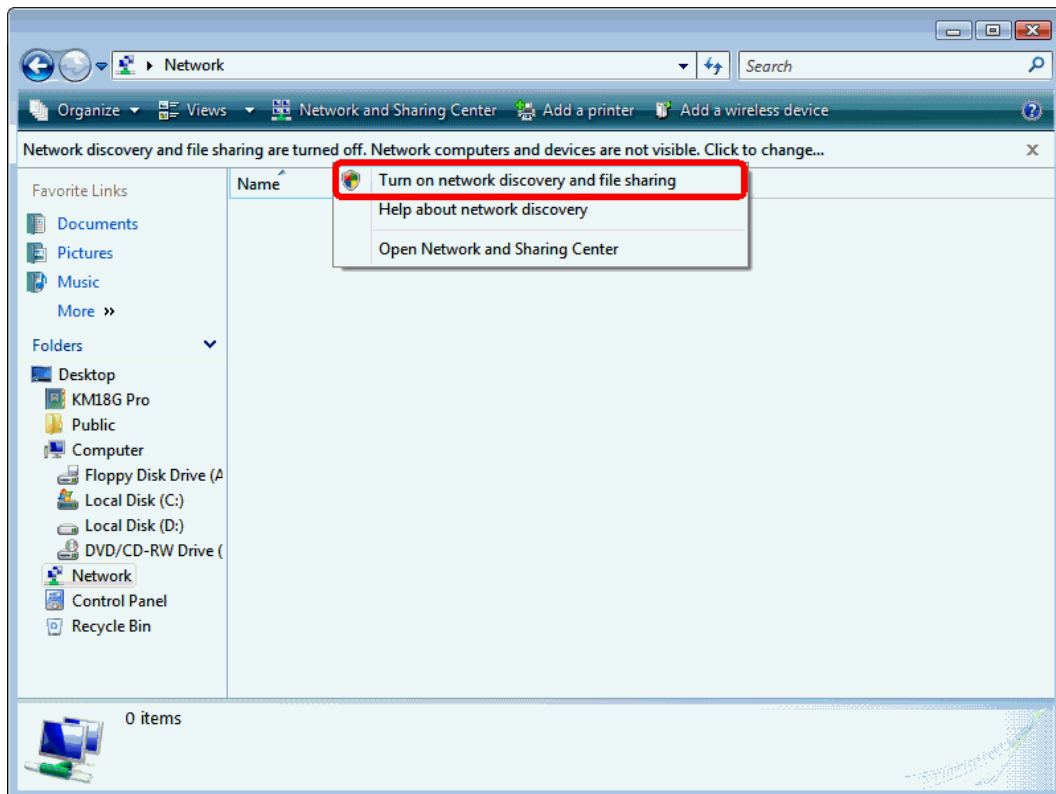
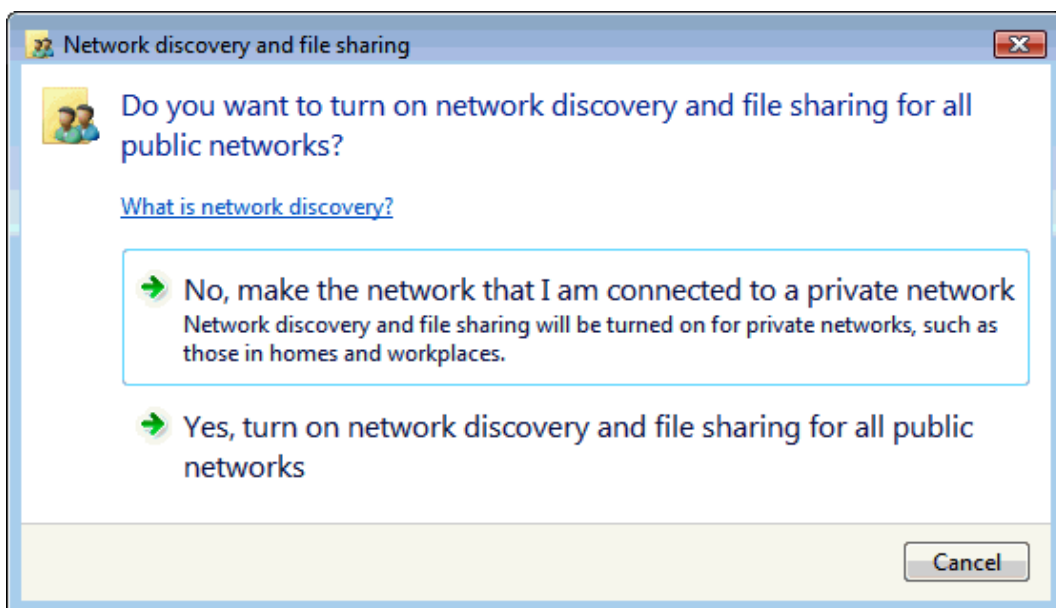
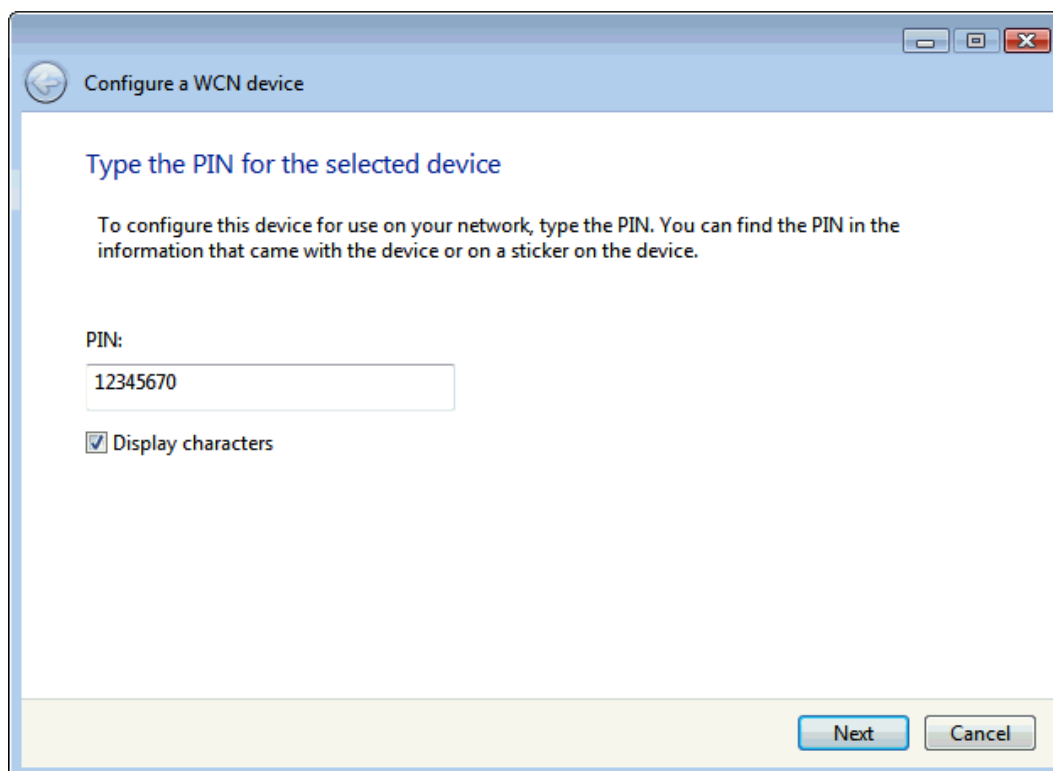
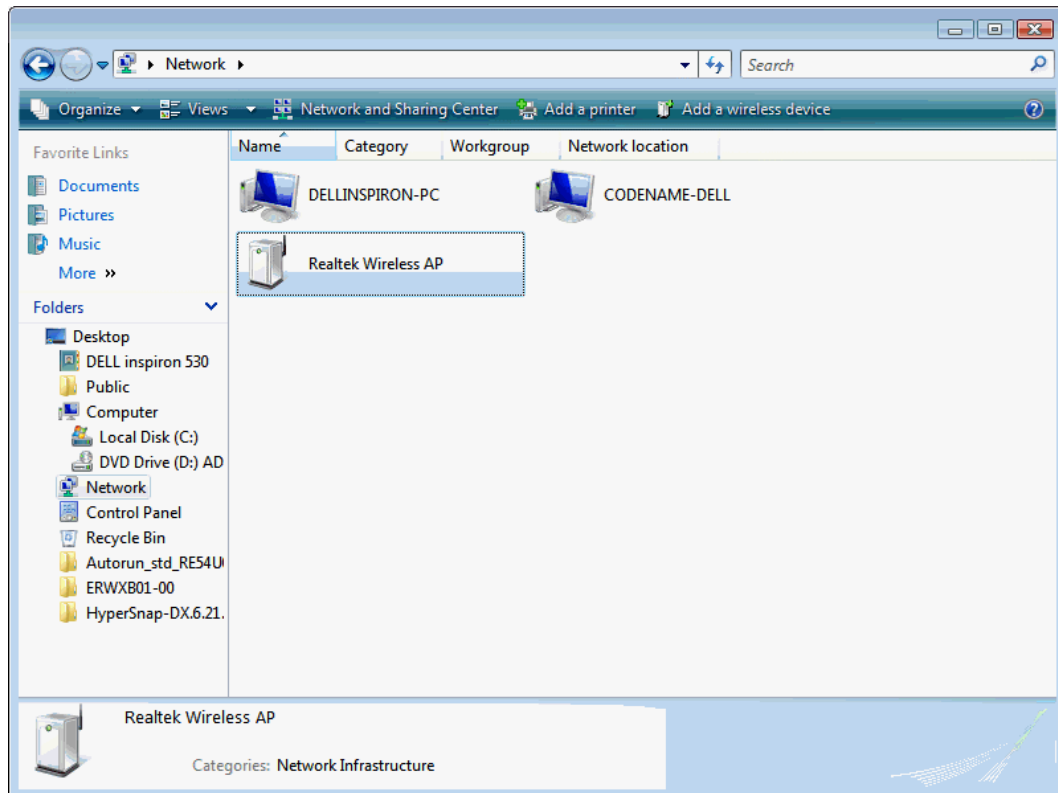
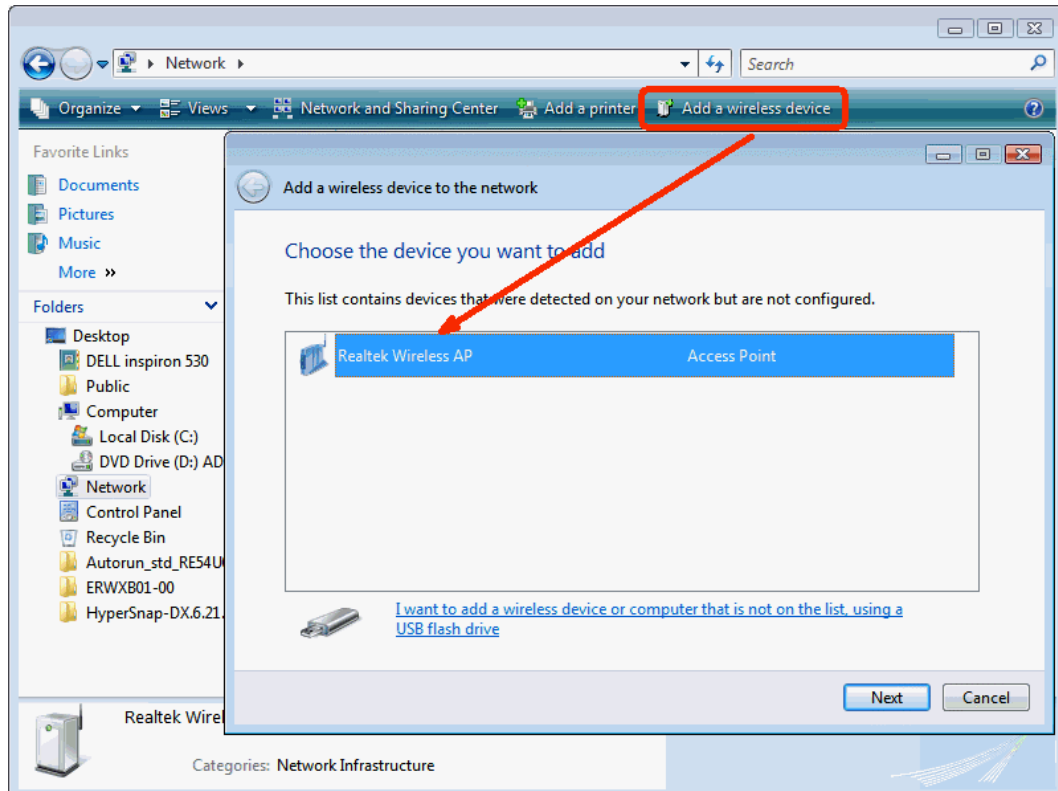
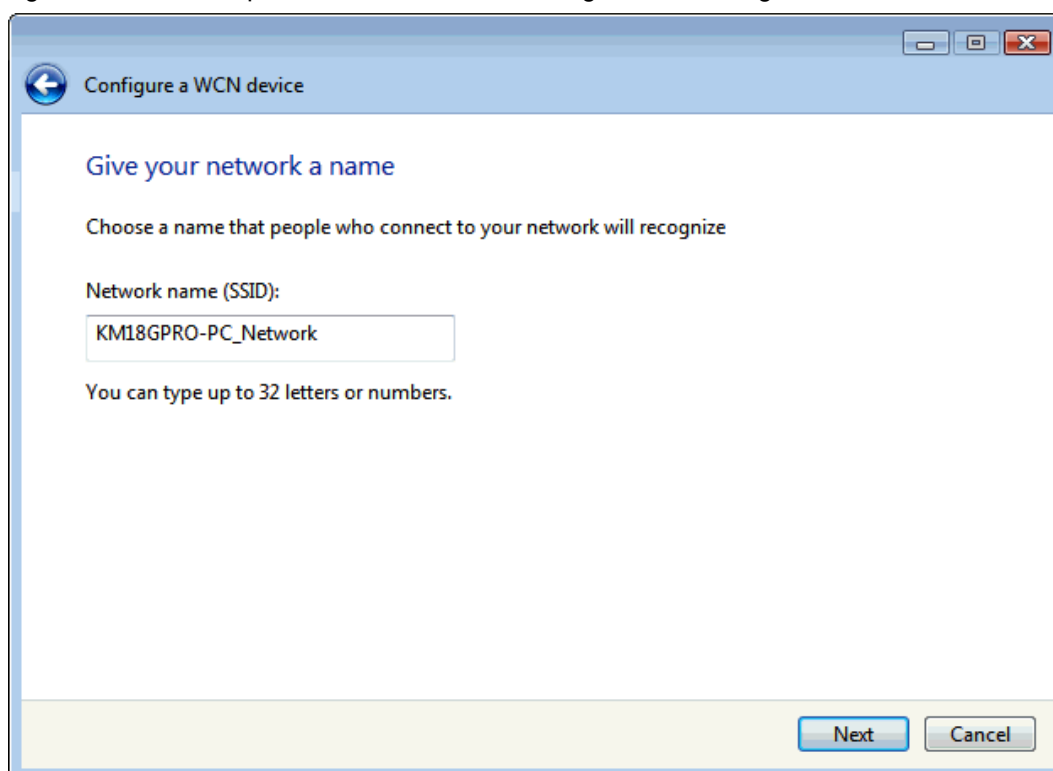
Apply Changes Reset

Current Key Info:

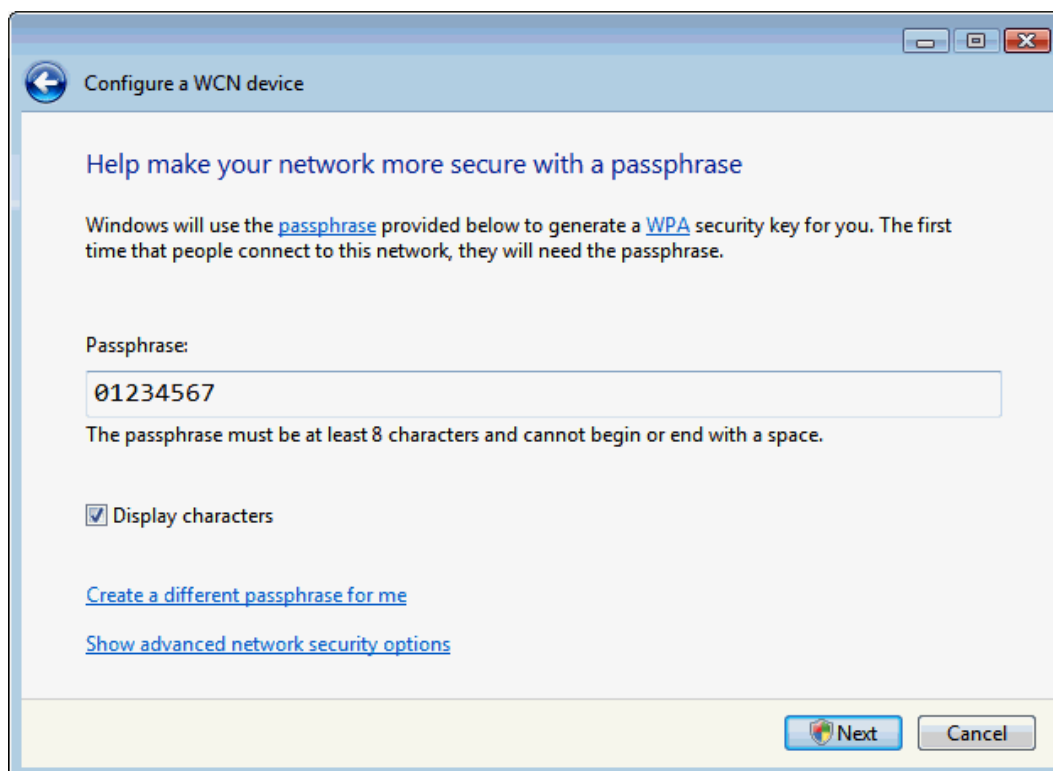
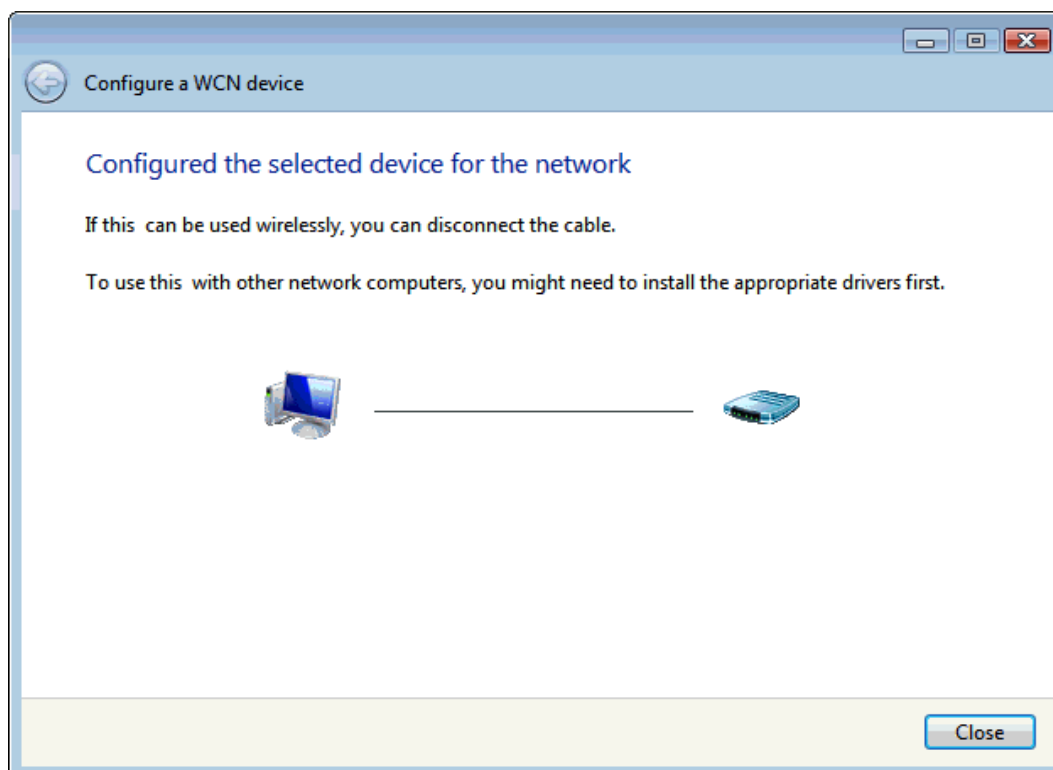
Authentication	Encryption	Key
Open	None	N/A

Client PIN Number: Start PIN

3. Inserite il cavo Ethernet nella porta LAN dell'Access Point e assicuratevi che la connessione IP sia valida per Vista.

4. Assicuratevi che la WCN sia abilitata. La prima volta gli utenti potrebbero aver bisogno di abilitarla. Questo è possibile aprendo il “Control Panel”, cliccare su “Classic View“, aprire “Administrative Tools”, fare doppio click su “Services”, verrà mostrata una finestra pop up, cliccare su “Continue“, modificare le proprietà di “Windows Connect Now”, impostare lo “Startup type” su “Automatic” e cliccare su “Start”.

5. Una volta completati i passi precedenti, aprite una finestra di Windows Explorer e andate alla sezione Network.
6. Cliccate su “Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to Change…“

7. Cliccate su “Turn on network discovery and file sharing“

8. Cliccate su “No, make the network that I am connected to a private network“

9. L'icona dell'Access Point comparirà, quindi fate doppio click sull'icona stessa.

10. Se non viene visualizzata l'icona, potete cliccare su “Add a wireless device”. Cliccate su “next”.

11. Inserite il codice PIN dell'Access Point e cliccate su "Next".

12. Scegliete un nome che possa essere riconoscibile dagli utenti che vogliono connettersi alla vostra rete.

13. Inserite la Password e cliccate su “Next”.

14. Comparirà una finestra pop up, cliccate su “Continue”.
15. L’access Point è stato configurato correttamente dal WCN.

16. L'Access Point è stato configurato (vedi "WPS Status"). L'algoritmo di autenticazione, l'algoritmo di crittografia e la chiave assegnata dal WCN verranno visualizzati sotto "Current Key Info".

17. Il campo dell'SSID della pagina *Wireless Basic Settings* verrà modificato con il valore assegnato dal WCN.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: AP Multiple AP

Network Type: Infrastructure

SSID: KM18GPRO-PC_Network

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

Associated Clients: Show Active Clients

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Apply Changes Reset

18. Le impostazioni di sicurezza nella pagina di *Wireless Security Setup* verranno modificate dal WCN. Un messaggio di allerta vi mostrerà se gli utenti cercheranno di modificare le impostazioni di sicurezza.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - DELLINSPIRON-PC_Network

Apply Changes Reset

Encryption: WPA

Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

WPA Cipher Suite: TKIP AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key: ●●●●●●●●●●●●●●●●●●●●●●

10.9 Operazioni dell'AP - AP come registrar

AP mode

Quando gli utenti inseriscono il PIN nella pagina si *Wi-Fi Protected Setup* dell'Access Point e cliccano su "Start PIN", l'Access Point diventerà un registrar. Gli utenti dovranno avviare il metodo PIN sulla stazione ricevente entro due minuti.

1. Dal menu *Wireless -> WPS,* verrà visualizzata la seguente pagina:
2. Assicuratevi che l'Access Point sia nello stato *UnConfigured*.
3. Inserite il *Client PIN Number*.
4. Cliccate su *Start PIN*.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

☐ **Disable WPS**

WPS Status: ○ Configured ◉ UnConfigured

Reset to UnConfigured

Self-PIN Number: 17843416

Push Button Configuration: Start PBC

Apply Changes Reset

Client PIN Number: 36866472 Start PIN

5. Gli utenti dovranno avviare il metodo PIN sulla stazione ricevente entro due minuti.

Applied client's PIN successfully!

You have to run Wi-Fi Protected Setup in client within 2 minutes.

6. Gli utenti dovranno avviare il metodo PIN sulla stazione ricevente entro due minuti.

7. Se il PIN del dispositivo è corretto e l'operazione sulla stazione ricevente è avvenuta con successo, verrà visualizzata la seguente finestra.

8. Se il PIN del dispositivo è corretto e l'operazione sulla stazione ricevente è avvenuta con successo, la pagina *Wi-Fi Protected Setup* dell'Access Point verrà visualizzata come di seguito:

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

☐ **Disable WPS**

WPS Status: ◉ Configured ○ UnConfigured

Reset to UnConfigured

Self-PIN Number: 17843416

Push Button Configuration: Start PBC

Apply Changes Reset

Current Key Info:

Authentication	Encryption	Key
WPA2-Mixed PSK	TKIP+AES	1a2cb3885d50987817fa5c

Client PIN Number: Start PIN

Metodo Push Button

Il Gateway Wireless supporta un tasto virtuale “Start PBC” nella pagina *Wi-Fi Protected Setup* per il metodo Push Button. Se gli utenti cliccano su questo tasto virtuale, l’Access Point avvierà una sessione WPS ed attenderà che tutte le stazioni vi si uniscano. A quel punto l’Access Point rileverà se ci sia più di una stazione che abbia avviato il metodo PBC. Quando questo accade, gli utenti dovranno provare con il metodo PIN.

Dopo che gli utenti avranno cliccato sul pulsante virtuale “Start PBC”, dovranno andare sulla stazione ricevente per premere il tasto entro due minuti. Se la WPS viene eseguita con successo, l’Access Point darà alla stazione il proprio profilo wireless.

1. Dal menu *Wireless* -> *WPS*, verrà visualizzata la seguente pagina:

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

- [ ] **Disable WPS**

WPS Status: ○ Configured ◉ UnConfigured

Reset to UnConfigured

Self-PIN Number: 17843416

Push Button Configuration: Start PBC

Apply Changes Reset

Client PIN Number: 36866472 Start PIN

2. Assicuratevi che l’Access Point sia nello stato *UnConfigured*.
3. Cliccate su *Start PBC*.
4. Gli utenti dovranno avviare il metodo PBC sulla stazione entro due minuti.

Start PBC successfully!

You have to run Wi-Fi Protected Setup in client within 2 minutes.

5. Gli utenti dovranno avviare il metodo PBC sulla stazione entro due minuti.

6. Se il PBC del dispositivo e l'operazione sulla stazione ricevente sono avvenuti con successo, verrà visualizzata la seguente finestra

7. Se il PBC del dispositivo e l'operazione sulla stazione ricevente sono avvenuti con successo, la pagina *Wi-Fi Protected Setup* dell'Access Point verrà visualizzata come di seguito.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

☐ **Disable WPS**

WPS Status: Configured UnConfigured

Reset to UnConfigured

Self-PIN Number: 17843416

Push Button Configuration: Start PBC

Apply Changes Reset

Current Key Info:

Authentication	Encryption	Key
WPA2-Mixed PSK	TKIP+AES	1a2cb3885d50987817fa5c

Client PIN Number: Start PIN

10.10 Pianificazione della Wireless

Questa pagina vi permette di pianificare l'uso dell'attività della funzione wireless. Ricordatevi di impostare l'orario di sistema prima di abilitare questa funzionalità. Per accedere alla pagina *Wireless Schedule*, dal menu *Wireless* sulla sinistra, cliccate su *Wireless Schedule*, verrà visualizzata la seguente pagina:

Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

Enable Wireless Schedule

Days :

Everyday Sun Mon Tue Wed Thu Fri Sat

Time :

24 Hours From 00 : 00 To 00 : 00

Apply Changes Reset

11. Interfaccia LAN

Questo capitolo serve a configurare i parametri per la connessione alla porta LAN del vostro Access Point. Qui è possibile cambiare le impostazioni per l'indirizzo IP, la subnet mask, il DHCP, etc.

***Nota**: Dovete cambiare queste impostazioni solo se il vostro ISP ve lo richiede o se comunque avete le necessarie conoscenze tecniche. In generale comunque non avrete bisogno di apportare modifiche.*

11.1 Configurazione dell'Interfaccia LAN

Per controllare la configurazione dell'interfaccia LAN:

1. Dal menu *Network Settings -> LAN Interface*, verrà visualizzata la seguente pagina:

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	10.0.0.2
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	10.0.0.100 - 10.0.0.200 Show Client
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Apply Changes Reset

Campo	Descrizione
IP Address	**L'indirizzo IP della LAN** **Default: 192.168.1.254**
Subnet Mask	**La netmask della LAN** **Default: 255.255.255.0**
Default Gateway	**Il Gateway della LAN** **Default: 0.0.0.0**
DHCP	**DHCP Type: Disable, DHCP Client o Server** **Default: DHCP Server**
DHCP Client Range	**Specifica l'indirizzo IP di inizio/fine del range.** **Default IP di inizio: 192.168.1.100** **Default IP di fine: 192.168.1.200**
Show Client	**I computer/dispositivi client DHCP connessi al dispositivo vedranno visualizzate le proprie informazioni nella DHCP Client List table.**
Domain Name	**Il nome associato all'indirizzo IP. Questo nome deve essere unico.**
802.1d Spanning Tree	**Abilita o Disabilita lo Spanning Tree**
Clone MAC Address	**MAC Spoofing della LAN** **Default: 000000000000**

11.2 Cambiare l'indirizzo IP della LAN e la subnet mask

Per controllare la configurazione dell'interfaccia LAN:

1. Dal menu *Network Settings -> LAN Interface*, verrà visualizzata la seguente pagina:

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	10.0.0.2
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	10.0.0.100 - 10.0.0.200 Show Client
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Apply Changes Reset

2. Digitate l'*IP Address* e *Change default LAN port IP address*.
3. Digitate nell'*IP Address and Subnet Mask* un nuovo Indirizzo IP e una Subnet Mask.
4. Cambiate il *default DHCP Client Range*.
5. Cliccate su *Apply Changes*.

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.2.2
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	192.168.2.100 - 192.168.2.200 Show Client
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

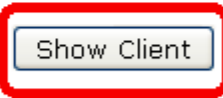
Apply Changes Reset

6. L'indirizzo IP primario viene modificato in 192.168.2.2 e la netmask in 255.255.255.0. Andate su http://192.168.2.2 per continuare. Il vostro browser comunica con il web server attraverso la connessione LAN e cambiare l'indirizzo IP potrebbe causare problemi

Change setting successfully!

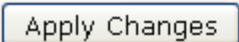
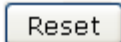
If IP address was modified, you have to re-connect the WebServer with the new address.

Potreste dover rinnovare il vostro DHCP:

Windows NT/Windows 2000/Windows XP

a. Aprite una finestra di comando.

b. Digitate il comando **ipconfig /release**.

c. Digitate **ipconfig /renew**.

d. Digitate **exit** per chiudere la finestra di comando.

11.3 Show Client

1. Dal menu *Network Settings -> LAN Interface*, verrà visualizzata la seguente pagina:

2. Cliccate su *Show Client*. Verrà visualizzata la seguente pagina:

12. Interfaccia WAN

Questo capitolo descrive come configurare la modalità di connessione del vostro dispositivo ad Internet. Il vostro ISP determina che tipo di accesso ad Internet dovreste usare e vi fornisce ogni informazione di cui avete bisogno per configurare la connessione ad Internet.

Il Gateway Wireless supporta cinque modalità per ottenere un indirizzo IP WAN.

OPZIONE	DESCRIZIONE
Static IP	**Scegliete questa opzione se siete un utente con una linea dedicata con indirizzo IP fisso.**
DHCP Client	**Scegliete questa opzione se siete connessi ad Internet attraverso una Cable modem line.**
PPPoE	**Scegliete questa opzione se siete connessi ad Internet con una linea DSL**
PPTP	**Scegliete questa opzione se siete connessi al Server PPTP**
L2TP	**Scegliete questa opzione se siete connessi al server L2TP**

1. Dal menu *Network Settings* -> *WAN Interface* verrà visualizzata la seguente pagina:

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Host Name:

MTU Size: 1492 (1400-1492 bytes)

Attain DNS Automatically

Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

Enable uPNP

Enable IGMP Proxy

Enable Ping Access on WAN

Enable Web Server Access on WAN

Enable IPsec pass through on VPN connection

Enable PPTP pass through on VPN connection

Enable L2TP pass through on VPN connection

Apply Changes Reset

OPZIONE		DESCRIZIONE
Tipo di accesso WAN	**Static IP**	**Scegliete questa opzione se siete un utente con una linea dedicata con indirizzo IP fisso.**
	DHCP Client	**Scegliete questa opzione se siete connessi ad Internet attraverso una Cable modem line.**
	PPPoE	**Scegliete questa opzione se siete connessi ad Internet con una linea DSL**
	PPTP	**Scegliete questa opzione se siete connessi al Server PPTP**
	L2TP	**Scegliete questa opzione se siete connessi al server L2TP**
Host Name		**Il nome dell'host DHCP**
IP Address		**Controllate con il vostro ISP**
Subnet Mask		**Controllate con il vostro ISP**
Default Gateway		**Controllate con il vostro ISP**
User Name		**Username per la registrazione PPPoE riconosciuta dall'ISP**
Password		**Password per la registrazione PPPoE riconosciuta dall'ISP**
Service Name		**Service Name per la registrazione PPPoE riconosciuto dall'ISP**
Tipo di connessione	**Continuous**	**Connessione sempre attiva**
	Connect on Demand	**Determinate dopo quanto tempo la sessione deve essere disconnessa, in assenza di attività**
	Manual	**Connessione manuale**
Idle Time		**Determinate dopo quanto tempo la sessione deve essere disconnessa**
WAN Physical		**IP dinamico o IP statico per la connessione PPP**
MTU Size		**Specificate il valore MTU della rete**
Attain DNS Automatically		**Ottenete automaticamente l'indirizzo del server DNS**
DNS 1 (Primary DNS Server)		**Controllate con il vostro ISP**
DNS 2 (Secondary DNS Server)		**Controllate con il vostro ISP**
DNS 3 (Third DNS Server)		**Controllate con il vostro ISP**

OPZIONE	DESCRIZIONE
Clone MAC Address	**Permette al dispositivo di identificarsi come un altro computer o dispositivo**
Enable UPnP	**Abilita/Disabilita l'UPnP**
Enable IGMP Proxy	**Abilita/Disabilita IGMP Proxy**
Enable Ping Access on WAN	**Abilita/Disabilita Ping Access on WAN**
Enable Web Server Access on WAN	**Abilita/Disabilita Web Server Access on WAN**
Enable IPsec pass through on VPN connection	**Abilita/Disabilita IPsec pass through on VPN connection**
Enable PPTP pass through on VPN connection	**Abilita/Disabilita PPTP pass through on VPN connection**
Enable L2TP pass through on VPN connection	**Abilita/Disabilita L2TP pass through on VPN connection**

12.1 Configurare la connessione con IP Statico

Se siete un utente con una linea dedicata con indirizzo IP fisso, inserite l'indirizzo IP, la subnet mask, l'indirizzo del gateway e l'indirizzo (o gli indirizzi) del DNS (domain name server) forniti dal vostro ISP.

Se il vostro ISP vuole che vi connettiate ad Internet con un indirizzo IP statico, seguite queste istruzioni:

1. Dal menu *Network Settings -> WAN Interface*, verrà visualizzata la seguente pagina:
2. Dal menu a tendina *WAN Access Type*, selezionate l'impostazione *Static IP*.
3. Inserite *WAN IP Address, WAN Subnet Mask, Default Gateway* e *DNS* che vi sono stati forniti dal vostro ISP.
4. Cliccate su *Apply Changes*.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: Static IP
IP Address: 172.1.1.1
Subnet Mask: 255.255.255.0
Default Gateway: 172.1.1.254
MTU Size: 1500 (1400-1500 bytes)
DNS 1: 172.1.1.254
DNS 2:
DNS 3:
Clone MAC Address: 000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Apply Changes Reset

5. Cliccate su *OK*.

Change setting successfully!

OK

6. Dal menu *Management -> Status*, verrà visualizzata la seguente pagina:
7. Se nel campo *Attain IP Protocol* viene mostrato ***Fixed IP***, potete già avere il vostro accesso ad Internet.

Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:7m:51s
Firmware Version	v1.4
Customer Version	REAN_v1.4_1T1R_STD_01_91106
Build Time	Fri Nov 6 17:48:33 CST 2009
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	11n_AP_Router
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:81:96:6a
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
Default Gateway	10.0.0.2
DHCP Server	Enabled
MAC Address	00:13:33:81:96:68
WAN Configuration	
Attain IP Protocol	Fixed IP Connected
IP Address	172.1.1.1
Subnet Mask	255.255.255.0
Default Gateway	172.1.1.254
MAC Address	00:13:33:81:96:69

12.2 Configurazione della connessione DHCP Client

Dynamic Host Configuration Protocol (DHCP), Dynamic IP (ottiene automaticamente l'indirizzo IP WAN). Se siete connessi ad Internet con una linea Cable modem, verrà assegnato un indirizzo IP dinamico.

Se il vostro ISP vuole che vi connettiate ad Internet con un DHCP Client, seguite queste istruzioni:

1. Dal menu *Network Settings -> WAN Interface*, verrà visualizzata la seguente pagina:
2. Dal menu a tendina *WAN Access Type*, selezionate l'impostazione *DHCP Client*.
3. Cliccate su *Apply Changes*.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client
Host Name:
MTU Size: 1492 (1400-1492 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection

Apply Changes Reset

4. Cliccate su *OK*.

Change setting successfully!

OK

5. Dal menu *Management -> Status*, verrà visualizzata la seguente pagina:
6. Se nel campo *Attain IP Protocol* viene mostrato ***DHCP***, potete già avere il vostro accesso ad Internet.

Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:14m:58s
Firmware Version	v1.4
Customer Version	REAN_v1.4_1T1R_STD_01_91106
Build Time	Fri Nov 6 17:48:33 CST 2009
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	11n_AP_Router
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:81:96:6a
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
Default Gateway	10.0.0.2
DHCP Server	Enabled
MAC Address	00:13:33:81:96:68
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.17
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
MAC Address	01:23:45:67:89:ab

12.3 Configurare la connessione PPPoE

Se il vostro ISP usa una PPPoE dovete impostare un account di login PPP. Alla prima connessione, il vostro ISP vi richiederà di inserire username e password, per verificare che siate effettivamente un utente registrato. Il vostro dispositivo immagazzina i dati di autenticazione e li ricorderà per i successivi accessi

Se il vostro ISP vuole che vi connettiate ad Internet usando un PPP, seguite queste istruzioni:

1. Dal menu *Network Settings -> WAN Interface*, verrà visualizzata la seguente pagina:
2. Dal menu a tendina *WAN Access Type*, selezionate l'impostazione *PPPoE*.
3. Inserite nei relativi campi *User Name/Password* forniti dal vostro ISP.
4. Cliccate su *Apply Changes*.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: PPPoE
User Name: 1234
Password: ••••
Service Name:
Connection Type: Continuous Connect Disconnect
Idle Time: 5 (1-1000 minutes)
MTU Size: 1452 (1360-1492 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection

Apply Changes Reset

5. Cliccate su *OK*.

Change setting successfully!

6. Dal menu *Management* -> *Status*, verrà visualizzata la seguente pagina:
7. Se nel campo *Attain IP Protocol* viene mostrato ***PPPoE Connected***, potete già avere il vostro accesso ad Internet.

Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:12m:32s
Firmware Version	v1.4
Customer Version	REAN_v1.4_1T1R_STD_01_91106
Build Time	Fri Nov 6 17:48:33 CST 2009
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	11n_AP_Router
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:81:96:6a
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
Default Gateway	10.0.0.2
DHCP Server	Enabled
MAC Address	00:13:33:81:96:6[illegible]
WAN Configuration	
Attain IP Protocol	PPPoE Connected
IP Address	192.168.10.106
Subnet Mask	255.255.255.255
Default Gateway	192.168.10.102
MAC Address	00:13:33:81:96:69

12.4 Configurare la connessione PPTP

Se il vostro ISP/Amministratore di Rete vuole che vi connettiate ad Internet con PPTP, seguite queste istruzioni:

1. Dal menu *Network Settings -> WAN Interface*, verrà visualizzata la seguente pagina:
2. Dal menu a tendina *WAN Access Type*, selezionate l'impostazione *PPTP*.
3. Inserite nei relativi campi *IP Address/Subnet Mask/Server IP Address/User Name/Password* forniti dal vostro ISP.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: PPTP
IP Address: 172.1.1.2
Subnet Mask: 255.255.255.0
Server IP Address: 172.1.1.1
User Name: 1234
Password: ●●●●
Connection Type: Continuous Connect Disconnect
Idle Time: 5 (1-1000 minutes)
MTU Size: 1460 (1400-1460 bytes)
Request MPPE Encryption Request MPPC Compression
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection

Apply Changes Reset

4. Cliccate su *Apply Changes*.
5. Cliccate su *OK*.

12.5 Configurare la connessione L2TP

Se il vostro ISP/Amministratore di Rete vuole che vi connettiate ad Internet con L2TP, seguite queste istruzioni:

1. Dal menu *Network Settings -> WAN Interface*, verrà visualizzata la seguente pagina:
2. Dal menu a tendina *WAN Access Type*, selezionate l'impostazione *L2TP*.
3. Inserite nei relativi campi *IP Address/Subnet Mask/Server IP Address/User Name/Password* forniti dal vostro ISP.
4. Cliccate su *Apply Changes*.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: L2TP
IP Address: 172.1.1.2
Subnet Mask: 255.255.255.0
Server IP Address: 172.1.1.1
User Name: 1234
Password: ●●●●
Connection Type: Continuous Connect Disconnect
Idle Time: 5 (1-1000 minutes)
MTU Size: 1460 (1400-1460 bytes)

Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 000000000000

Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection

Apply Changes Reset

5. Cliccate su *OK*.

Change setting successfully!

OK

12.6 Clonare l'Indirizzo MAC

Alcuni particolari ISP non vi permettono di avere una rete domestica e hanno solo un DSL/Cable modem che vi consente solo un MAC. Se cambiate le schede di rete, dovete cambiare gli indirizzi MAC.

Questa pagina vi permette di abilitare o disabilitare l'opzione *Clone MAC Address:*

1. Dal menu *Network Settings -> WAN Interface*, verrà visualizzata la seguente pagina:
2. Inserite l'indirizzo MAC nel campo *Clone MAC Address*, ad esempio 0123456789ab.
3. Se inserite 12 zeri nel campo *Clone MAC Address*, la funzione *Clone MAC Address* verrà disabilitata.
4. Cliccate su *Apply Changes*.

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Host Name:

MTU Size: 1492 (1400-1492 bytes)

Attain DNS Automatically

Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 0123456789ab

Enable uPNP

Enable IGMP Proxy

Enable Ping Access on WAN

Enable Web Server Access on WAN

Enable IPsec pass through on VPN connection

Enable PPTP pass through on VPN connection

Enable L2TP pass through on VPN connection

Apply Changes Reset

5. Cliccate su *OK*.

Change setting successfully!

OK

6. Dal menu *Management -> Status*, verrà visualizzata la seguente pagina:
7. Nel campo *WAN Configuration -> MAC Address* potete vedere se compare l'indirizzo MAC che avete inserito.

Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:14m:58s
Firmware Version	v1.4
Customer Version	REAN_v1.4_1T1R_STD_01_91106
Build Time	Fri Nov 6 17:48:33 CST 2009
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	11n_AP_Router
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:81:96:6a
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
Default Gateway	10.0.0.2
DHCP Server	Enabled
MAC Address	00:13:33:81:96:68
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.17
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
MAC Address	01:23:45:67:89:ab

13. Port Filtering

I valori in *Current Filter Table* vengono usati per limitare alcune porte e tipi di pacchetti di dati dalla rete locale ad Internet attraverso il Gateway. L'uso di tali filtri è utile nel rendere più sicura la vostra rete.

1. Dal menu *Firewall -> Port Filtering*, verrà visualizzata la seguente pagina:

Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Port Filtering

Port Range: - Protocol: Both Comment:

Apply Changes Reset

Current Filter Table:

Port Range	Protocol	Comment	Select

Delete Selected Delete All Reset

Opzione	Descrizione
Enable Port Filtering	**Abilita/Disabilita il filtro del pacchetto WAN.** **Valore preimpostato: Disabilitato.**
Port Range	**Inserite il range da filtrare sia per i pacchetti in entrata che in uscita**
Protocol	**Selezionate il Protocollo da filtrare sia per i pacchetti in entrata che per quelli in uscita.** **Entrambi: Per filtrare sia il protocollo TCP che quello UDP** **TCP: Per filtrare solo il protocollo TCP** **UDP: Per filtrare solo il protocollo UDP**
Comment	**Inserite un commento sulla funzionalità della regola di filtering**
Current Filter Table	**I filtri che sono stati creati vengono elencati in questa tabella**

***Nota**: Assicuratevi che la singola porta o il range di porte specificati non si sovrappongano con porte o range un'applicazione già esistente.*

13.1 Port filtering per la porta 80 TCP

Seguite le seguenti istruzioni per negare la porta 80 TCP ai pacchetti sia in entrata che in uscita:

1. Dal menu *Firewall -> Port Filtering*, verrà visualizzata la seguente pagina:

Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ **Enable Port Filtering**

Port Range: [ ] - [ ] **Protocol:** Both **Comment:** [ ]

Apply Changes | Reset

Current Filter Table:

Port Range	Protocol	Comment	Select

Delete Selected | Delete All | Reset

2. Selezionate l'opzione *Enable Port Filtering* per abilitare il port filtering.
3. Inserite *80* e *80* nel campo *Port Range*.
4. Dal menu a tendina *Protocol*, selezionate l'impostazione *TCP*.
5. Inserite HTTP nel campo *Comment*.
6. Cliccate su *Apply Changes*.

7. Ora il filtro che avete creato è stato aggiunto ed elencato in *Current Filter Table*.
8. Ora la porta TCP viene negata sia ai pacchetti in entrata che a quelli in uscita.

Current Filter Table:

Port Range	Protocol	Comment	Select
80	TCP	HTTP	☐

Delete Selected | Delete All | Reset

E' quindi impossibile visitare alcun sito web a causa della regola di Port Filtering che è stata creata.

13.2 Port filtering per la porta 53 UDP

Seguite le seguenti istruzioni per negare la porta 53 UDP ai pacchetti sia in entrata che in uscita:

1. Dal menu *Firewall -> Port Filtering*, verrà visualizzata la seguente pagina:

Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ **Enable Port Filtering**

Port Range: [ ] - [ ] **Protocol:** Both **Comment:** [ ]

Apply Changes | Reset

Current Filter Table:

Port Range	Protocol	Comment	Select

Delete Selected | Delete All | Reset

2. Selezionate l'opzione *Enable Port Filtering* per abilitare il port filtering.
3. Inserite *53* e *53* nel campo *Port Range*.
4. Dal menu a tendina *Protocol*, selezionate l'impostazione *UDP*.
5. Inserite DNS Resolve nel campo *Comment*.
6. Cliccate su *Apply Changes*.

7. Ora il filtro che avete creato è stato aggiunto ed elencato in *Current Filter Table*.
8. Ora la porta UDP viene negata sia ai pacchetti in entrata che a quelli in uscita.

Current Filter Table:

Port Range	Protocol	Comment	Select
53	UDP	DNS Resolve	☐

Delete Selected | Delete All | Reset

E' quindi impossibile visitare alcun sito web a causa della regola di Port Filtering che è stata creata.

You can enter the IP Address of that web site to visit.

14. IP Filtering

I valori in questa tabella vengono usati per limitare alcune porte e tipi di pacchetti di dati dalla rete locale ad Internet attraverso il Gateway. L'uso di tali filtri è utile nel rendere più sicura la vostra rete.

La funzione di IP filtering vi permette di creare regole di controllo sui dati in entrata e in uscita tra la LAN e la WAN.

Potete creare regole che blocchino i tentativi di accesso a determinati tipi di dati o indirizzi Internet da parte di alcuni computer. Potete anche bloccare l'accesso ai computer della LAN da parte della WAN.

Quando definite una regola di filtro e abilitate la funzione, comunicate al router di esaminare i pacchetti di dati per determinare se combacino con i criteri specificati nella regola. I criteri possono comprendere il protocollo Internet o di rete, il trasferimento dei pacchetti, la loro direzione di trasferimento (ad esempio, dalla LAN alla WAN e viceversa).

Se il pacchetto combacia con i criteri stabiliti in una regola, il pacchetto può essere sia accettato che rifiutato, a seconda dell'azione specificata nella regola.

La pagina di configurazione dell'IP Filter fornisce la possibilità di abilitare/disabilitare la funzionalità di filtro ed i valori di filtro per ogni regola stabilita.

1. Dal menu *Firewall -> IP Filtering*, verrà visualizzata la seguente pagina:

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ **Enable IP Filtering**

Loal IP Address: [ ] **Protocol:** Both **Comment:** [ ]

Apply Changes | Reset

Current Filter Table:

Local IP Address	Protocol	Comment	Select

Delete Selected | Delete All | Reset

14.1 IP filtering per TCP con IP specifico

Seguite queste istruzioni per negare il protocollo TCP per un IP specifico:

1. Dal menu *Firewall -> IP Filtering*, verrà visualizzata la seguente pagina:

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering

Loal IP Address: Protocol: Both Comment:

Apply Changes Reset

Current Filter Table:

Local IP Address	Protocol	Comment	Select

Delete Selected Delete All Reset

2. Selezionate l'opzione *Enable Port Filtering* per abilitare l'IP Filtering.
3. Inserite l'indirizzo IP cui volete negare l'accesso campo *Loal IP Address*.
4. Dal menu a tendina *Protocol*, selezionate l'impostazione *TCP*.
5. Inserite un commento nel campo *Comment*.
6. Cliccate su *Apply Changes*.

7. Ora il filtro IP che avete creato è stato aggiunto ed elencato in *Current Filter Table*.
8. Ora la porta TCP viene negata sia ai pacchetti in entrata che a quelli in uscita.

Quindi ora l'indirizzo IP locale (ad esempio 10.0.0.102) che è elencato nella *Current Filter Table* non può visitare alcuna applicazione che usi il protocollo TCP.

14.2 IP filtering per UDP con IP specifico

Seguite queste istruzioni per negare il protocollo UDP per un IP specifico:

1. Dal menu *Firewall -> IP Filtering*, verrà visualizzata la seguente pagina:

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ Enable IP Filtering

Loal IP Address: Protocol: Both Comment:

Apply Changes Reset

Current Filter Table:

Local IP Address	Protocol	Comment	Select

Delete Selected Delete All Reset

2. Selezionate l'opzione *Enable Port Filtering* per abilitare l'IP Filtering.
3. Inserite l'indirizzo IP cui volete negare l'accesso nel campo *Loal IP Address*.
4. Dal menu a tendina *Protocol*, selezionate l'impostazione *UDP*.
5. Inserite un commento nel campo *Comment*.
6. Cliccate su *Apply Changes*.

7. Ora il filtro IP che avete creato è stato aggiunto ed elencato in *Current Filter Table*.
8. Ora la porta UDP viene negata sia ai pacchetti in entrata che a quelli in uscita.

Current Filter Table:

Local IP Address	Protocol	Comment	Select
10.0.0.102	UDP	Deny UDP	☐

Delete Selected Delete All Reset

Quindi ora l'indirizzo IP locale (ad esempio 10.0.0.102) che è elencato nella *Current Filter Table* non può visitare alcuna applicazione che usi il protocollo UDP.

14.3 IP filtering sia per TCP che UDP con IP specifico

Seguite queste istruzioni per negare i protocolli TCP e UDP per un IP specifico:

1. Dal menu *Firewall -> IP Filtering*, verrà visualizzata la seguente pagina:

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ **Enable IP Filtering**

Loal IP Address: [ ] **Protocol:** Both **Comment:** [ ]

Apply Changes | Reset

Current Filter Table:

Local IP Address	Protocol	Comment	Select

Delete Selected | Delete All | Reset

2. Selezionate l'opzione *Enable Port Filtering* per abilitare l'IP Filtering.
3. Inserite l'indirizzo IP cui volete negare l'accesso campo *Loal IP Address*.
4. Dal menu a tendina *Protocol*, selezionate l'impostazione *Both*.
5. Inserite un commento nel campo *Comment*.
6. Cliccate su *Apply Changes*.

7. Ora il filtro IP che avete creato è stato aggiunto ed elencato in *Current Filter Table*.
8. Ora le porte TCP e UDP vengono negate sia ai pacchetti in entrata che a quelli in uscita.

Current Filter Table:

Local IP Address	Protocol	Comment	Select
10.0.0.102	TCP+UDP	Deny TCP+UDP	☐

Delete Selected | Delete All | Reset

15. MAC Filtering

I valori in questa tabella vengono usati per limitare alcune porte e tipi di pacchetti di dati dalla rete locale ad Internet attraverso il Gateway. L'uso di tali filtri è utile nel rendere più sicura la vostra rete.

1. Dal menu *Firewall -> MAC Filtering*, verrà visualizzata la seguente pagina:

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ **Enable MAC Filtering**

MAC Address: ______ **Comment:** ______

[Apply Changes] [Reset]

Current Filter Table:

MAC Address	Comment	Select

[Delete Selected] [Delete All] [Reset]

15.1 MAC filtering per un indirizzo MAC specifico

Seguite queste istruzioni per negare l'accesso ad Internet ad un indirizzo MAC specifico.

1. Dal menu *Firewall -> MAC Filtering*, verrà visualizzata la seguente pagina:

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ **Enable MAC Filtering**

MAC Address: [ ] **Comment:** [ ]

[Apply Changes] [Reset]

Current Filter Table:

MAC Address	Comment	Select

[Delete Selected] [Delete All] [Reset]

2. Selezionate l'opzione *Enable MAC Filtering* per abilitare il MAC Filtering.
3. Inserite l'indirizzo MAC al quale volete negare l'accesso nel campo *MAC Address*.
4. Inserite un commento nel campo *Comment*.
5. Cliccate su *Apply Changes*.

☑ **Enable MAC Filtering**

MAC Address: 000a48122926 **Comment:** Test

[Apply Changes] [Reset]

Current Filter Table:

MAC Address	Comment	Select

[Delete Selected] [Delete All] [Reset]

6. Ora il filtro MAC che avete creato è stato aggiunto ed elencato in *Current Filter Table*.
7. Ora l'indirizzo MAC nel *Current Filter Table* non ha accesso ad Internet

Current Filter Table:

MAC Address	Comment	Select
00:0a:48:12:29:26	Test	☐

[Delete Selected] [Delete All] [Reset]

16. Port Forwarding

I valori in questa tabella vi permettono di reindirizzare automaticamente servizi della rete ad una macchina specifica oltre il firewall del NAT.

Se volete semplicemente connettervi ad Internet dalla vostra rete locale, non dovete apportare alcuna modifica alla configurazione preimpostata della sicurezza. Dovete apportare delle modifiche solo nel caso in cui vogliate:

- Permettere agli utenti di Internet di navigare le pagine sulla vostra rete locale (ad esempio fornendo un server FTP o HTTP)
- Fare alcuni giochi che necessitano l'accessibilità da Internet

Questo capitolo descrive come configurare la sicurezza per soddisfare le necessità della vostra rete.

Come valore predefinito, gli indirizzi IP dei computer della vostra LAN sono nascosti. Tutti i dati inviati appariranno quindi come provenienti dall'indirizzo IP del vostro dispositivo.

In questo modo, i dettagli dei PC della vostra LAN resteranno privati. Questa funzione di sicurezza è chiamata *Port Forwarding*.

1. Dal menu *Firewall -> Port Forwarding*, verrà visualizzata la seguente pagina:

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☐ **Enable Port Forwarding**

IP Address: ___ **Protocol:** Both **Port Range:** ___ - ___ **Comment:** ___

Apply Changes | Reset

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Delete Selected | Delete All | Reset

16.1 Port Forwarding per TCP con IP specifico

Seguite queste istruzioni per configurare il Port Forwarding ad un indirizzo IP con TCP.

1. Dal menu *Firewall -> Port Forwarding*, verrà visualizzata la seguente pagina:

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☐ **Enable Port Forwarding**

IP Address: **Protocol:** Both **Port Range:** - **Comment:**

Apply Changes Reset

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Delete Selected Delete All Reset

2. Selezionate l'opzione *Enable Port Forwarding* per abilitare il Port Forwarding.
3. Inserite l'indirizzo IP della porta nel campo *IP Address*.
4. Dal menu a tendina *Protocol*, selezionate l'impostazione *TCP*.
5. Inserite un commento nel campo *Comment*.
6. Cliccate su *Apply Changes*.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☑ **Enable Port Forwarding**

IP Address: 10.0.0.101 **Protocol:** TCP **Port Range:** 80 - 80 **Comment:** Test

Apply Changes Reset

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Delete Selected Delete All Reset

7. Ora l'indirizzo IP e il range di porte che avete creato sono stati aggiunti ed elencati in *Current Filter Table*.
8. Ora si può accedere al range di porte nel *Current Filter Table* attraverso il protocollo TCP.

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
10.0.0.101	TCP	80	Test	☐

Delete Selected Delete All Reset

16.2 Port Forwarding per UDP con IP specifico

Seguite queste istruzioni per configurare il Port Forwarding ad un indirizzo IP con UDP.

1. Dal menu *Firewall -> Port Forwarding*, verrà visualizzata la seguente pagina:

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☐ Enable Port Forwarding

IP Address: Protocol: Both Port Range: - Comment:

Apply Changes Reset

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Delete Selected Delete All Reset

2. Selezionate l'opzione *Enable Port Forwarding* per abilitare il Port Forwarding.
3. Inserite l'indirizzo IP della porta nel campo *IP Address*.
4. Dal menu a tendina *Protocol*, selezionate l'impostazione *UDP*.
5. Inserite un commento nel campo *Comment*.
6. Cliccate su *Apply Changes*.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☑ Enable Port Forwarding

IP Address: 10.0.0.101 Protocol: UDP Port Range: 69 - 69 Comment: Test

Apply Changes Reset

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Delete Selected Delete All Reset

7. Ora l'indirizzo IP e il range di porte che avete creato sono stati aggiunti ed elencati in *Current Filter Table*.
8. Ora si può accedere al range di porte nel *Current Filter Table* attraverso il protocollo UDP.

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
10.0.0.101	UDP	69	Test	☐

Delete Selected Delete All Reset

17. URL Filtering

Il filtro URL viene usato per negare l'accesso ad Internet da parte degli utenti della LAN. Potete bloccare quegli URL che contengono le parole elencate:

1. Dal menu *Firewall -> URL Filtering*, verrà visualizzata la seguente pagina:

URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

Enable URL Filtering

URL Address:

Apply Changes Reset

Current Filter Table:

URL Address	Select

Delete Selected Delete All Reset

17.1 URL filtering per un indirizzo URL specifico

Seguite queste istruzioni per configurare il Port Forwarding ad un indirizzo IP con UDP.

1. Dal menu *Firewall -> URL Filtering*, verrà visualizzata la seguente pagina:

URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

☐ **Enable URL Filtering**

URL Address:

Apply Changes | Reset

Current Filter Table:

URL Address	Select

Delete Selected | Delete All | Reset

2. Selezionate l'opzione *Enable URL Filtering* per abilitare l'URL Filtering.
3. Inserite l'indirizzo URL cui volete negare l'accesso.
4. Cliccate su *Apply Changes*.

URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

☑ **Enable URL Filtering**

URL Address: www.google.com

Apply Changes | Reset

Current Filter Table:

URL Address	Select

Delete Selected | Delete All | Reset

5. Ora il filtro URL che avete creato è stato aggiunto ed elencato in *Current Filter Table*.
6. Ora l'indirizzo URL nel *Current Filter Table* non può essere visitato

Current Filter Table:

18. DMZ

Una Demilitarized Zone viene usata per fornire servizi Internet senza sacrificare un accesso non autorizzato alla propria rete locale. Di solito li DMZ host contiene dispositivi per il traffico Internet, quali Web (HTTP) server, FTP server, SMTP (e-mail) server and DNS server.

1. Dal menu *Firewall -> DMZ*, verrà visualizzata la seguente pagina:

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

☐ **Enable DMZ**

DMZ Host IP Address:

Apply Changes Reset

18.1 Indirizzo IP del DMZ Host

Seguite queste istruzioni per configurare l'indirizzo IP del DMZ host.

2. Dal menu *Firewall -> DMZ*, verrà visualizzata la seguente pagina:

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

3. Selezionate l'opzione *Enable DMZ* per abilitare il DMZ.
4. Inserite l'indirizzo IP che deve fungere da DMZ host nel campo *DMZ Host IP Address*.
5. Cliccate su *Apply Changes*.

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

6. Cliccate su *OK*.

Change setting successfully!

OK

19. VLAN

Gli elementi di questa tabella vengono usati per configurare le impostazioni della VLAN. Le VLAN vengono create per fornire i servizi di segmentazione tradizionalmente forniti dai router. Le VLAN indirizzano regole quali scalabilità, sicurezza e gestione della rete.

1. Dal menu *Firewall -> VLAN*, verrà visualizzata la seguente pagina:

VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

☐ **Enable VLAN**

Enable	Ethernet/Wireless	WAN/LAN	Tag	VID (1~4090)	Priority	CFI
☐	Ethernet Port1	LAN	☐	3022	7	☑
☐	Ethernet Port2	LAN	☐	3030	0	☑
☐	Ethernet Port3	LAN	☐	500	3	☑
☐	Ethernet Port4	LAN	☐	1	0	☑
☐	Wireless Primary AP	LAN	☐	1	0	☑
☐	Virtual AP1	LAN	☐	1	0	☑
☐	Virtual AP2	LAN	☐	1	0	☑
☐	Virtual AP3	LAN	☐	1	0	☑
☐	Virtual AP4	LAN	☐	1	0	☑
☐	Ethernet Port5	WAN	☐	1	0	☑

Apply Changes   Reset

20. QoS

Gli elementi di questa tabella migliorano la vostra capacità di giocare online assicurando che a questo traffico venga data la priorità sul resto del traffico della rete.

2. Dal menu *Firewall -> QoS*, verrà visualizzata la seguente pagina:

QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

☐ Enable QoS

☑ Automatic Uplink Speed

Manual Uplink Speed (Kbps): 512

☐ Automatic Downlink Speed

Manual Downlink Speed (Kbps): 0

QoS Rule Setting:

Address Type: ◉ IP ○ MAC

Local IP Address: -

MAC Address:

Mode: Guaranteed minimum bandwidth

Uplink Bandwidth (Kbps):

Downlink Bandwidth (Kbps):

Comment:

Apply Changes Reset

Current QoS Rules Table:

Local IP Address	MAC Address	Mode	Uplink Bandwidth	Downlink Bandwidth	Comment	Select

Delete Selected Delete All Reset

21. Stato

Questa pagina mostra le attuali informazioni del dispositivo, tra cui le informazioni sulla LAN, WAN e firmware del sistema. Questa pagina mostrerà diverse informazioni, in base alle impostazioni della WAN (Static IP, DHCP, o PPPoE).

1. Dal menu *Management* -> *Status*, verrà visualizzata la seguente pagina:

Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:13h:32m:43s
Firmware Version	v1.4
Customer Version	REAN_v1.4_1T1R_STD_02_91229
Build Time	Tue Dec 29 19:16:36 CST 2009
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	11n_AP_Router
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:81:96:4f
Associated Clients	1
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
Default Gateway	10.0.0.2
DHCP Server	Enabled
MAC Address	00:13:33:81:96:4d
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.42
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
MAC Address	00:13:33:81:96:4e

22. Statistiche

Questa pagina mostra i contatori dei pacchetti inviati e ricevuti per le reti wireless ed Ethernet.

1. Dal menu *Management* -> *Statistics*, verrà visualizzata la seguente pagina:

Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	*Sent Packets*	135
	Received Packets	31439
Ethernet LAN	*Sent Packets*	5748
	Received Packets	5560
Ethernet WAN	*Sent Packets*	1840
	Received Packets	4385

Refresh

23. DNS dinamico

Quando volete che si possa accedere al vostro server interno usando il DNS piuttosto che l'indirizzo IP dinamico, potete usare il servizio DDNS. Questo servizio vi permette di aggiornare l'indirizzo IP dinamico

1. Dal menu *Management* -> *DDNS*, verrà visualizzata la seguente pagina:

Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☐ **Enable DDNS**

Service Provider : DynDNS

Domain Name : host.dyndns.org

User Name/Email:

Password/Key:

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

Apply Change   Reset

23.1 Configurare il DynDNS

1. Dal menu *Management* -> *DDNS*, verrà visualizzata la seguente pagina:

Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS

Service Provider : DynDNS
Domain Name : host.dyndns.org
User Name/Email:
Password/Key:

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

Apply Change Reset

2. Cliccate su *Enable DDNS*
3. Selezionate il DynDNS dal menu a tendina *Service Provider*.
4. Digitate nei relativi campi *User Name*, *Password* e *Domain Name*. Possono essere ogni combinazione di lettere o numeri, fino ad un massimo di 20 caratteri.
5. Cliccate su *Apply Changes*.

Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS

Service Provider : DynDNS
Domain Name : villiamcheng.dyndns.org
User Name/Email: williamcheng
Password/Key: ●●●●●●●●●

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

Apply Change Reset

6. Cliccate su *OK*.

Change setting successfully!

OK

23.2 Configurare il TZO

1. Dal menu *Management* -> *DDNS*, verrà visualizzata la seguente pagina:

Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS

Service Provider : DynDNS
Domain Name : host.dyndns.org
User Name/Email:
Password/Key:

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

Apply Change Reset

2. Cliccate su *Enable DDNS*
3. Selezionate il TZO dal menu a tendina *Service Provider*.
4. Inserite nei relativi campi i vostri *Email*, *Key* e *Domain Name*. Possono essere ogni combinazione di lettere o numeri, fino ad un massimo di 20 caratteri.
5. Cliccate su *Apply Changes*.

Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS

Service Provider : TZO
Domain Name :
User Name/Email:
Password/Key:

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

Apply Change Reset

6. Cliccate su *OK*.

Change setting successfully!

OK

24. Impostazioni Time Zone

Alcuni sistemi possono non avere un meccanismo per la data o l'ora, o possono usare informazioni non corrette. La funzione Simple Network Time Protocol fornisce un modo per sincronizzare questi valori del dispositivo, impostando un orario remoto come descritto in RFC 2030 (SNTP) e RFC 1305 (NTP).

Configurare SNTP Server e SNTP Client

1. Dal menu *Management*, cliccate su *Time Zone Setting*, verrà visualizzata la seguente pagina:

Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr 2009 Mon 12 Day 29 Hr 20 Mn 12 Sec 4

Copy Computer Time

Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana

Enable NTP client update

Automatically Adjust Daylight Saving

NTP server : 192.5.41.41 - North America

(Manual IP Setting)

Apply Change Reset Refresh

2. Dal menu a tendina *Time Zone Select*, selezionate *Your Own Time Zone*.
3. Selezionate l'opzione *Enable NTP client update*.
4. Dal menu a tendina *NTP server*, selezionate un *NTP Server*. Oppure potete aggiungere un server all'elenco di associazione SNTP usando l'indirizzo IP: automaticamente partirà il processo di sincronizzazione.
5. Cliccate su *Apply Changes*.
6. Cliccate su *OK*.

Change setting successfully!

OK

25. Denial-of-Service

Un attacco "denial-of-service" (DoS) è caratterizzato da un tentativo esplicito da parte di hacker di impedire agli utenti di utilizzare un servizio.

1. Dal menu *Management* cliccate su *Denial-of-Service*, verrà visualizzata la seguente pagina:

Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

Enable DoS Prevention

Whole System Flood: SYN	0	Packets/Second
Whole System Flood: FIN	0	Packets/Second
Whole System Flood: UDP	0	Packets/Second
Whole System Flood: ICMP	0	Packets/Second
Per-Source IP Flood: SYN	0	Packets/Second
Per-Source IP Flood: FIN	0	Packets/Second
Per-Source IP Flood: UDP	0	Packets/Second
Per-Source IP Flood: ICMP	0	Packets/Second
TCP/UDP PortScan	Low	Sensitivity
ICMP Smurf		
IP Land		
IP Spoof		
IP TearDrop		
PingOfDeath		
TCP Scan		
TCP SynWithData		
UDP Bomb		
UDP EchoChargen		

Select ALL Clear ALL

Enable Source IP Blocking 0 Block time (sec)

Apply Changes

2. Selezionate l'opzione *Enable NTP client update*.
3. Selezionate l'opzione di ogni *Service*.
4. Selezionate l'opzione *Enable Source IP Blocking*.
5. Cliccate su *Apply Changes*.

Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

☑ Enable DoS Prevention

☑	Whole System Flood: SYN	0	Packets/Second
☑	Whole System Flood: FIN	0	Packets/Second
☑	Whole System Flood: UDP	0	Packets/Second
☑	Whole System Flood: ICMP	0	Packets/Second
☑	Per-Source IP Flood: SYN	0	Packets/Second
☑	Per-Source IP Flood: FIN	0	Packets/Second
☑	Per-Source IP Flood: UDP	0	Packets/Second
☑	Per-Source IP Flood: ICMP	0	Packets/Second
☑	TCP/UDP PortScan	Low	Sensitivity
☑	ICMP Smurf		
☑	IP Land		
☑	IP Spoof		
☑	IP TearDrop		
☑	PingOfDeath		
☑	TCP Scan		
☑	TCP SynWithData		
☑	UDP Bomb		
☑	UDP EchoChargen		

Select ALL Clear ALL

☑ Enable Source IP Blocking 0 Block time (sec)

Apply Changes

6. Cliccate su *OK*.

Change setting successfully!

OK

26. Log

Questa pagina può essere usata per impostare un server di registro remoto e mostrare il registro di sistema.

Registro di sistema

1. Dal menu *Management*, cliccate su *Log*, verrà visualizzata la seguente pagina:

System Log

This page can be used to set remote log server and show the system log.

Enable Log

system all wireless DoS 11s

Enable Remote Log Log Server IP Address:

Apply Changes

Refresh Clear

Opzione	Descrizione
Enable Log	**Abilita/Disabilita la funzione.** **Preimpostato: Disabilitato**
system all	**Tutti i registri di sistema verranno mantenuti nel registro di sistema**
wireless	**I registri della wireless verranno mantenuti nel registro di sistema**
DoS	**I registri di DoS verranno mantenuti nel registro di sistema**
Enable Remote Log	**Abilitato: Invia il registro di sistema al server di registro remoto** **Preimpostato: Disabilitato**
Log Server IP Address	**Inserite l'Indirizzo IP del server di registro remoto.**

2. Selezionate l'opzione *Enable Log*.
3. Selezionate l'opzione *system all, wireless* or *DoS*.
4. Selezionate l'opzione *Enable Remote Log*.
5. Inserite l'"indirizzo IP nel campo *Log Server IP Address*.
6. Cliccate su *Apply Changes*.

System Log

This page can be used to set remote log server and show the system log.

Enable Log
system all wireless DoS 11s
Enable Remote Log Log Server IP Address: 10.0.0.100

Apply Changes

Refresh Clear

7. Cliccate su *OK*.

Change setting successfully!

OK

27. Aggiornamento del Firmware

27.1 Versioni del firmware

Il Firmware è un programma software e viene registrato sul vostro dispositivo come memoria di sola lettura. Hamletcom migliora continuamente questo firmware aggiungendo nuove funzionalità, le quali vengono salvate in successive versioni del firmware.

Il vostro dispositivo può controllare se ci sia una nuova versione disponibile ed in questo caso potete scaricarla su Internet ed installarla sul vostro dispositivo.

***Nota**: Se c'è un aggiornamento del firmware, è altamente consigliato installarla sul vostro dispositivo.*

27.2 Aggiornare manualmente il firmware

Potete scaricare manualmente la versione più recente del firmware dal sito web: www.hamletcom.com.

Una volta scaricata, potete selezionarla direttamente dal vostro PC ed installarla come segue:

1. Dal menu *Management*, cliccate su *Upgrade Firmware*, verrà visualizzata la seguente pagina:
2. Cliccate su *Browse*….

Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

(Se state usando alcuni browser come *Opera 7*, il tasto *Browse* sarà etichettato come *Choose*.)

Usate *Choose file* per selezionare la directory dove è salvata la versione del firmware.

3. Una volta selezionato il file da installare, cliccate su *Open*. Il percorso del file viene visualizzato in *New Firmware Image:*.
4. Cliccate su *Upgrade* >. Il dispositivo verifica che il file selezionato contenga una versione aggiornata del firmare. Comparirà una finestra pop up che vi avviserà di attendere.

5. L'aggiornamento del Firmware è stato completato. Verrà visualizzata la seguente pagina:
6. Cliccate su *OK*.

Update successfully (size = 1855196 bytes)!

Please wait a while for rebooting...

OK

28. Impostazioni Save/Reload

Questa pagina vi permette di salvare le attuali impostazioni su file o di reimpostare quelle precedentemente salvate.

Inoltre, potete reimpostare le configurazioni di fabbrica effettuando il reset.

28.1 Salvare le Impostazioni su File

Vi permette di salvare le attuali impostazioni su file:

1. Dal menu *Management*, cliccate su *Reset factory default*. Verrà visualizzata la seguente pagina:

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.

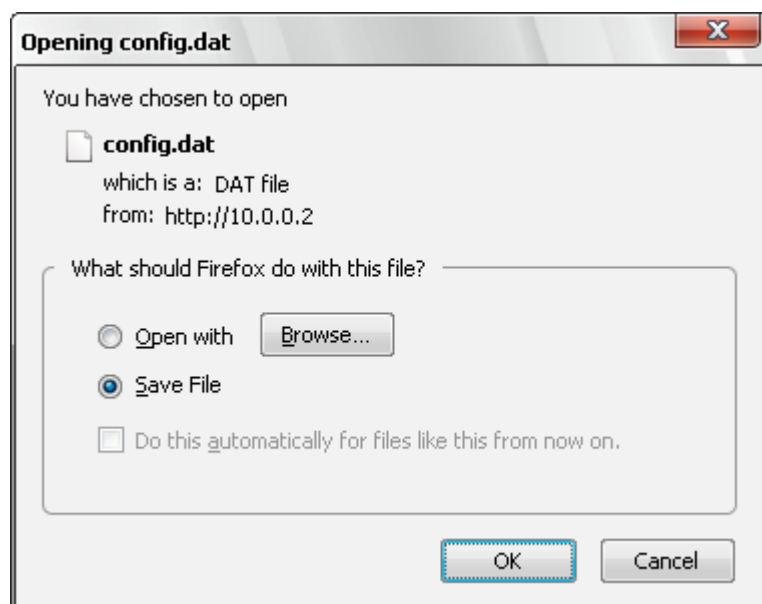
Save Settings to File: Save...

Load Settings from File: Browse... Upload

Reset Settings to Default: Reset

Opzione	Descrizione
Save Settings to File	**Salva le impostazioni VoIP su file**
Load Settings from File	**Carica le impostazioni da file**
Reset Settings to Default	**Reimposta i valori VoIP di fabbrica**

2. Cliccate su *Save…*.

3. Cliccate su *OK* e selezionate il percorso su cui salvare il file. Oppure cliccate su *Cancel* per annullare.

28.2 Caricare le Impostazioni da File

Vi permette di ricaricare le impostazioni dal file precedentemente salvato.

1. Dal menu *Management*, cliccate su *Reset factory default*. Verrà visualizzata la seguente pagina:

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.

Save Settings to File: Save...

Load Settings from File: Browse... Upload

Reset Settings to Default: Reset

2. Cliccate su *Browse…*.per selezionare il file.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.

Save Settings to File: Save...

Load Settings from File: Browse... Upload

Reset Settings to Default: Reset

3. Cliccate su *Upload* per avviare il caricamento delle impostazioni da file.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.

Save Settings to File: Save...

Load Settings from File: iron 530\Desktop\config.dat Browse... Upload

Reset Settings to Default: Reset

4. Una volta terminata l'operazione, verrà visualizzato il messaggio seguente.

Update successfully!

OK

28.3 Reimpostare i valori di default

***Nota**: Se reimpostate i valori di fabbrica del vostro dispositivo, tutte le modifiche precedenti verranno perse*

Reset del Software:

1. Dal menu *Management*, cliccate su *Reset factory default*. Verrà visualizzata la seguente pagina:

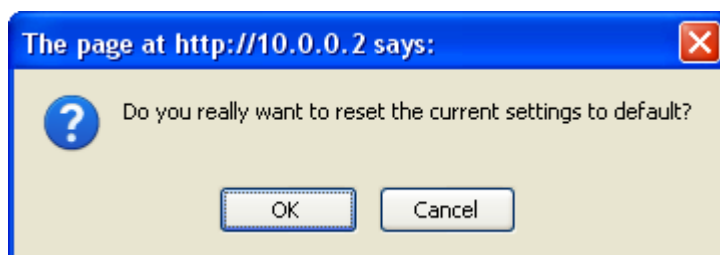
Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.

2. Cliccate su *Reset Settings to Default*.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.

3. Questa pagina vi ricorda che la reimpostazione dei valori di fabbrica non può essere annullata. Quando cliccate su *OK* verranno sostituite tutte le precedenti impostazioni. Cliccando su *Cancel* verrà annullata l'operazione.

4. L'operazione di reload è stata effettuata con successo. Attendete mentre viene effettuato il riavvio...

Reload setting successfully!

Please wait for a moment while rebooting ...

5. Al termine dell'operazione verrà visualizzata la pagina Status.

Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:14m:58s
Firmware Version	v1.4
Customer Version	REAN_v1.4_1T1R_STD_01_91106
Build Time	Fri Nov 6 17:48:33 CST 2009
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	11n_AP_Router
Channel Number	11
Encryption	Disabled
BSSID	00:13:33:81:96:6a
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
Default Gateway	10.0.0.2
DHCP Server	Enabled
MAC Address	00:13:33:81:96:68
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.17
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
MAC Address	01:23:45:67:89:ab

29. Password

Potete restringere l’accesso alle pagine web attraverso l’uso di una password. L’utente deve quindi inserire username e password per poter accedere alle pagine web.

La protezione con password è abilitata per default sul vostro dispositivo e i valori sono i seguenti:

Username: **admin**

Password: **hamlet**

29.1 Impostare username e password

***Note**: E’ altamente consigliato cambiare username e password predefinite con vostri valori*

Per cambiare la password predefinita:

1. Dal menu *Management*, cliccate su *Password*. Verrà visualizzata la seguente pagina:

Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:

New Password:

Confirmed Password:

Apply Changes Reset

2. Questa pagina mostra le attuali impostazioni di username e password. Cambiate i valori dei rispettivi campi, che possono essere combinazioni di lettere e numeri per un massimo di 30 caratteri.
3. Per rendere effettive le modifiche, cliccate su ***Apply***.

Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name: root

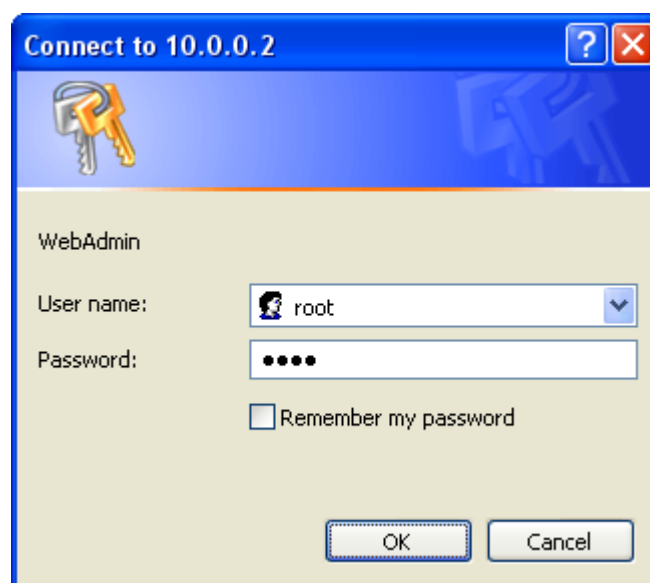
New Password: ••••

Confirmed Password: ••••

Apply Changes Reset

4. Cliccate su *OK*.

Change setting successfully!

5. Inserite i nuovi *Username* e *Password*.
6. Cliccate su *Apply*.

30. Logout

Per effettuare il logout:

1. Dal menu cliccate su *Logout*. Verrà visualizzata la seguente pagina:
2. Cliccate su *Apply Change*.

Logout

This page is used to logout.

Do you want to logout ?

Apply Change

Configurare i vostri Computer

Questa appendice fornisce istruzioni per configurare le impostazioni Internet sul vostro computer per lavorare con il Gateway Wireless.

Configurare PC Ethernet

Prima di iniziare

Per default, il Gateway Wireless assegna automaticamente ai vostri PC le impostazioni Internet richieste. Dovete configurare i PC per accettare queste informazioni quando vengono assegnate.

Se avete connesso i PC della LAN via Ethernet al Gateway Wireless, seguite le seguenti istruzioni:

PC Windows® XP

1. Nella barra degli indirizzi di Windows, cliccate su *Start*, quindi cliccate su *Control Panel*.
2. Fate doppio click sull'icona *Network Connections*.
3. Nella finestra *LAN or High-Speed Internet*, fate click con il tasto destro sull'icona corrispondente alla vostra scheda di rete (NIC) e selezionate *Properties*. (altrimenti etichettata come *Local Area Connection*).
4. La finestra di dialogo *Local Area Connection* visualizzerà un elenco di elementi di rete attualmente installati.
5. Assicuratevi che la check box alla voce *Internet Protocol TCP/IP* sia selezionata e cliccate su *Properties*.
6. Nella finestra di dialogo *Internet Protocol (TCP/IP) Properties*, selezionate l'opzione *Obtain an IP address automatically*. Selezionate inoltre l'opzione *Obtain DNS server address automatically*.
7. Cliccate due volte su *OK* per confermare le modifiche, quindi chiudete il *Control Panel*.

B Indirizzi IP, Network Mask e Subnet

Indirizzi IP

Nota: *Questa sezione fa riferimento solo agli indirizzi IP per IPv4 (versione 4 del Protocollo Internet). Non sono trattati gli indirizzi IPv6.*

Questa sezione presume una conoscenza base dei numeri binari e del concetto di bit/byte.

Gli indirizzi IP sono utilizzati per identificare nodi individuali (computer o dispositivi) su Internet. Ogni indirizzo IP è costituito da quattro numeri, con valore da 0 a 255 e separati da un punto, come ad esempio 20.56.0.211. Questi numeri sono chiamati, da sinistra a destra, campo1, campo2, campo3 e campo4.

Questo modo di scrivere gli indirizzi IP viene definito *dotted decimal notation*. L'indirizzo IP 20.56.0.211 si legge "venti punto cinquantasei punto zero punto duecentoundici".

Struttura di un indirizzo IP

Gli indirizzi IP hanno una struttura gerarchica simile a quella dei numeri di telefono. Ad esempio, un numero telefonico di 7 cifre inizia con un prefisso di 3 cifre che identifica un gruppo di migliaia di linee telefoniche, e finisce con 4 cifre che identificano una specifica linea in quel gruppo.

In modo analogo, gli indirizzi IP contengono due tipi di informazioni:

- *ID di rete*
  Identifica una rete particolare in Internet o Intranet
- *ID dell'host*
  Identifica un computer o un dispositivo particolari sulla rete

La prima parte di ogni indirizzo IP contiene l'ID di rete e il resto dell'indirizzo contiene l'ID dell'host. La lunghezza dell'ID di rete dipende dalla classe della rete (vedi la sezione successiva). La tabella seguente mostra la struttura di un indirizzo IP.

	Campo1	Campo2	Campo3	Campo4
Class A	ID di rete	ID dell'host		
Class B	ID di rete		ID dell'host	
Class C	ID di rete			ID dell'host

Qui ci sono degli esempi di indirizzi IP validi:

Classe A: 10.30.6.125 (rete = 10, host = 30.6.125)
Classe B: 129.88.16.49 (rete = 129.88, host = 16.49)
Classe C: 192.60.201.11 (rete = 192.60.201, host = 11)

Classi di rete

Le tre classi di rete comunemente usate sono A, B e C (c'è anche una classe D ma ha un'utilità speciale al di là dello scopo di questa sezione). Queste classi hanno usi e caratteristiche diversi.

Le reti di classe A sono le reti più estese di Internet, ciascuna con spazio per più di 16 milioni di host. Possono esistere fino a 126 di queste ampie reti, per un totale di più di 2 bilioni di host. Proprio per la loro enorme grandezza, queste reti vengono usate per le WAN e da organizzazioni a livello di infrastruttura di Internet, come ad esempio il tuo ISP.

Le reti di classe B sono più piccole ma comunque abbastanza estese, ognuna capace di contenere più di 65,000 host. Qui possono esserci più di 16,384 reti di classe B. Una rete di classe B può essere adatta per una grande organizzazione come enti governativi o di commercio.

Le reti di classe C sono le più piccole, capaci di contenere al più 254 host, ma il numero totale di reti di classe C va oltre i 2 milioni (esattamente 2,097,152). Le LAN usualmente connesse ad Internet sono di classe C.

Alcune importanti note riguardanti gli indirizzi IP:

- La classe può essere facilmente determinata dal campo1:
  campo1 = 1-126: Classe A
  campo1 = 128-191: Classe B
  campo1 = 192-223: Classe C
  (i valori del campo1 non mostrati sono riservati per usi speciali)
- Un ID dell'host può avere ogni valore eccetto l'impostazione di tutti i campi a 0 o 255, come quei valori riservati per usi speciali.

Subnet mask

Definizione: *Una mask appare come un indirizzo IP regolare, ma contiene un percorso di bit che spiega quali parti di un indirizzo IP sono ID di rete e quali ID di host: bit impostati ad 1 significano "questo bit è parte dell'ID di rete" e bit impostati a 0 significano "questo bit è parte dell'ID dell'host".*

Le *Subnet mask* sono usate per definire le *sottoreti* (quelle che ottieni dopo aver diviso una rete in pezzi più piccoli). Un ID di rete per la sottorete viene creato "affittando" uno o più bit dalla porzione di indirizzo dell'ID dell'host. La subnet mask identifica questi bit dell'ID host.

Ad esempio, considera una rete di classe C 192.168.1. Per suddividerla in due sottoreti, dovresti usare la subnet mask:

255.255.255.128

E' più facile vedere cosa sta succedendo se lo scriviamo in binario:

11111111. 11111111. 11111111.10000000

Come per ogni indirizzo di classe C, tutti i bit nel campo1 fino al campo3 sono parte dell'ID di rete, ma nota come la mask specifichi che il primo bit nel campo4 è anch'esso incluso. Finché questo extra bit ha solo due valori (0 e 1), significa che ci sono due sottoreti. Ogni sottorete usa i restanti 7 bit del campo4 per i propri ID di host, che variano da 1 a 126 host (invece dei soliti da 0 a 255 per un indirizzo di classe C).

Analogamente, per dividere una rete di classe C in quattro sottoreti, la mask è:

255.255.255.192 o 11111111. 11111111. 11111111.11000000

I due bit extra nel campo4 possono avere 4 valori (00, 01, 10, 11), così da avere quattro sottoreti. Ogni sottorete usa i restanti sei bit del campo4 per i propri ID di host, che variano da 1 a 62.

Nota: *A volte una subnet mask non specifica alcun bit di ID di rete addizionale, quindi alcuna sottorete. Tale mask viene detta default subnet mask. Queste mask sono:*

Classe A: 255.0.0.0
Classe B: 255.255.0.0
Classe C: 255.255.255.0

Queste sono dette di default perché vengono usate quando una rete è inizialmente configurata, quando cioè non ha ancora sottoreti.

C UPnP Control Point Software per Windows XP

Questa appendice fornisce istruzioni per la configurazione dell'UPnP sui vostri computer per lavorare con il Gateway Wireless.

L'UPnP è un'architettura per la connettività di reti peer-to-peer di apparecchi intelligenti, dispositivi wireless e PC di ogni marca. E' progettato per consentire una connettività flessibile, semplice da usare e standardizzata, attraverso reti domestiche, in ufficio o in spazi aperti.

L'UPnP è pensato per permettere una interconnessione senza configurazione e con il rilevamento automatico di nuovi dispositivi. Ciò significa che un dispositivo può unirsi alla rete in modo dinamico, ottenere un indirizzo IP e comunicare con gli altri dispositivi. Allo stesso modo può lasciare la rete senza causare effetti indesiderati al resto della rete.

UPnP Control Point Software per Windows XP con Firewall

Nelle versioni di Windows XP precedenti a SP2, il supporto Firewall viene fornito dal Windows XP Internet Connection Firewall. Non potete usare questo supporto su di un sistema che volete usare come UPnP control point.

Su Windows XP SP2 e versioni successive, il supporto Firewall viene fornito dal Windows Firewall. A differenza delle versioni precedenti, Windows XP SP2 può anche essere usato su di un sistema che volete usare come UPnP control point.

Per spegnere la funzionalità Firewall seguite questi passi (per ogni versione di Windows XP):

1. Nel "Control Panel", selezionate "Network and Internet Connections".

2. In "Network and Internet Connections", selezionate "Network Connections".

3. In "Network Connections", fate click con il tasto destro sull'elemento di connessione alla vostra rete locale; verrà visualizzato un menu. Selezionate "Properties".

4. In "Local Area Connection Properties", selezionate "Advanced". Disabilitate il Firewall della connessione Internet deselezionando l'elemento con questa etichetta:"Protect my computer and network by limiting or preventing access to the computer from the Internet".

5. Cliccate su "OK".

Requisiti SSDP

Dovete avere SSDP Discovery Service abilitato sul vostro sistema con Windows XP per poter usare l'UPnP Control point software.

SSDP Discovery Service è abilitato nell'installazione predefinita di Windows XP. Per controllare che sia abilitato sul vostro sistema, verificate su Control Panel > Administrative Tools > Services).

Procedura di installazione

Per installare il Control point software su Windows XP, seguite questi passi:

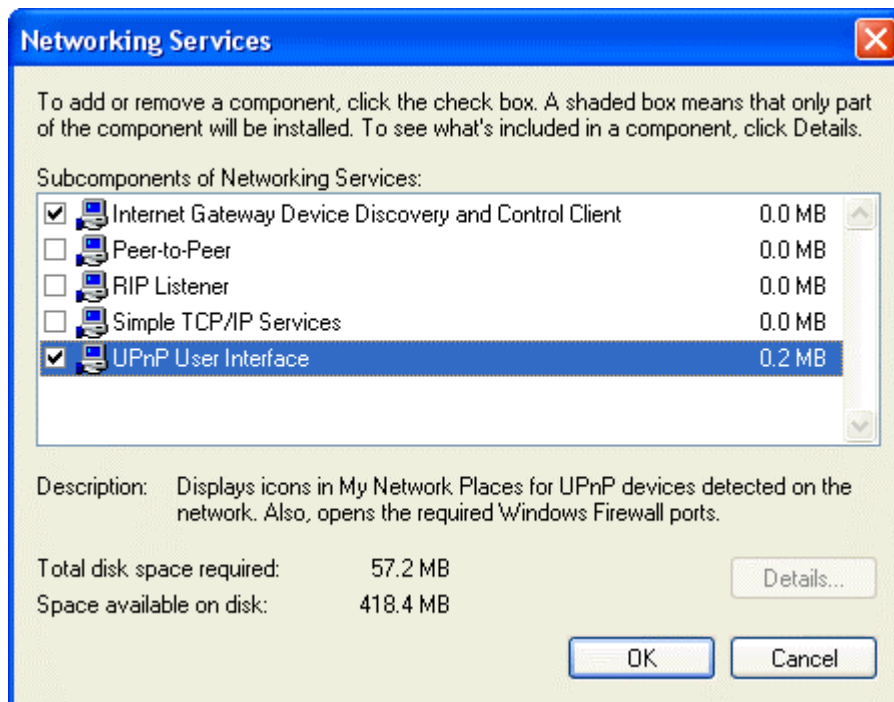
1. In "Control Panel", selezionate "Add/Remove Programs".

2. In "Add or Remove Programs", cliccate su "Add / Remove Windows Components".

3. In "Windows Component Wizard", scorrete la lista fino all'elemento "Networking Services". Selezionatelo e cliccate su "Details".

4. Verrà visualizzata la finestra "Networking Services".

Le sottocomponenti mostrate in "Networking Services" saranno diverse in base al fatto che stiate usando Windows XP, Windows XP (SP1), o Windows XP (SP2).

Se state usando Windows XP SP2, in “Networking Services” verranno visualizzate le seguenti sottocomponenti:

5. Selezionate i seguenti elementi da “Networking Services” e cliccate su "OK":

Se state usando **Windows XP**, selezionate:

- "Universal Plug and Play".

Se state usando **Windows XP SP1**, selezionate:

- "Internet Gateway Device discovery and Control Client".
- "Universal Plug and Play".

Se state usando **Windows XP SP2**, selezionate:

- "Internet Gateway Device discovery and Control Client".
- "UPnP User Interface".

6. Riavviate il sistema.

Una volta installato il software UPnP e riavviato il sistema, dovreste poter vedere il dispositivo Gateway sulla vostra rete.

Risoluzione dei Problemi

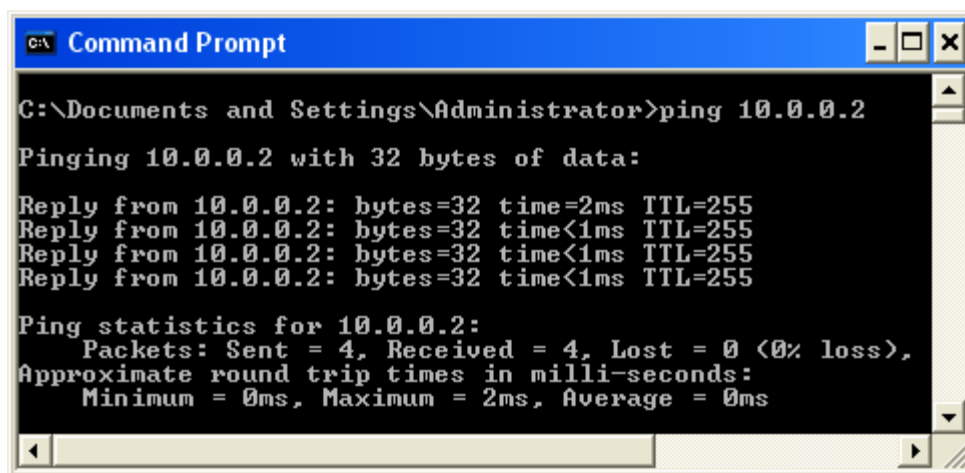
Questa appendice suggerisce soluzioni per problemi che potreste incontrare quando installate o usate il Gateway Wireless e fornisce istruzioni sull’uso di varie funzioni IP per risolvere i problemi.

Se questi suggerimenti non vi aiutano nella risoluzione del problema, contattate il Supporto Clienti.

Suggerimenti per la risoluzione dei problemi

Problema	Suggerimento di risoluzione
LED	
Il Power LED non si illumina dopo aver acceso il dispositivo	Assicuratevi che l’adattatore del dispositivo sia collegato al dispositivo ed inserito in una presa funzionante. Utilizzate solo l’adattatore in dotazione.
Il LED del collegamento LAN non si illumina dopo aver attaccato il cavo Ethernet.	Verificate che il cavo Ethernet sia correttamente connesso al PC (o hub) e al Gateway. Assicuratevi che il PC e/o l’hub siano accesi. Verificate che il cavo soddisfi i requisiti della rete.
Accesso Internet	
Il mio PC non riesce ad accedere ad Internet.	Usate la funzione ping per controllare se il vostro PC riesca a comunicare con l’indirizzo IP della LAN del dispositivo (per default 192.168.1.254). Se non ci riesce, controllate il cablaggio Ethernet. Se avete assegnato staticamente un indirizzo IP al computer: • Controllate che l’indirizzo IP del Gateway sul computer sia il vostro indirizzo IP pubblico. Altrimenti correggete l’indirizzo o configurate il PC per ricevere automaticamente informazioni riguardo l’IP. • Verificate con il vostro ISP che il DNS server specificato per il PC sia valido. Correggete l’indirizzo o configurate il PC per ricevere automaticamente queste informazioni.
I PC della mia LAN non riescono a visualizzare pagine web su Internet.	Verificate che l’indirizzo IP del DNS server specificato sui PC sia corretto per il vostro ISP. Se avete specificato che il DNS server fosse assegnato dinamicamente da un server, verificate con il vostro ISP che l’indirizzo impostato sul Gateway Wireless sia corretto, quindi potete usare la funzione ping per testare la connettività con il DNS server del vostro ISP.
Pagine Web	
Ho dimenticato nome utente e/o password.	Se non avete cambiato i valori preimpostati, provate ad usare “admin” per il nome utente e “hamlet“ per la password. Altrimenti potete fare il reset del dispositivo per reimpostare i valori di default, premendo il tasto di Reset sul pannello posteriore del dispositivo. Quindi digitate il nome utente e la password predefiniti. **ATTENZIONE:** Effettuando il reset del dispositivo, verranno rimosse tutte le impostazioni personalizzate e le modifiche apportate.
Non riesco ad accedere alle pagine web dal mio browser.	Usate la funzione ping per controllare se il vostro PC riesca a comunicare con l’indirizzo IP della LAN del dispositivo (per default 192.168.1.254). Se non ci riesce, controllate il cablaggio Ethernet. Verificate di usare Internet Explorer o Netscape Navigator v4.0 o successive. Verificate che l’indirizzo IP del PC sia definito nella stessa sottorete dell’indirizzo IP assegnato alla porta della LAN sul Gateway Wireless.
Le mie modifiche alle pagine web non sono state mantenute.	Assicuratevi di usare la funzione *Confirm Changes/Apply in seguito ad ogni modifica apportata*.

Diagnosticare il problema con le utility IP

ping

potete usare il comando *Ping* per verificare se il vostro PC riesca a riconoscere altri computer sulla vostra rete e su Internet. Un comando ping invia un messaggio al computer che avete specificato. Se il computer riceve il messaggio, vi invierà un messaggio di risposta. Per usare questa funzionalità dovete però conoscere l'indirizzo IP del computer con il quale state cercando di comunicare.

Sui computer con sistema operativo Windows, potete eseguire questo comando cliccando su *Start*, quindi su *Run*. Digitate quindi un comando come questo:

ping 192.168.1.254

Cliccate su *OK*.

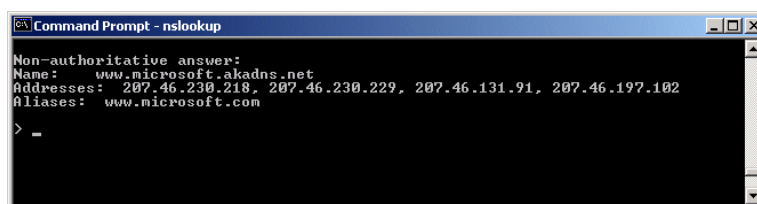
Se il computer di destinazione riceve il messaggio, verrà visualizzata la finestra *Command Prompt*:

```
Command Prompt

C:\Documents and Settings\Administrator>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=2ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Se il computer non può invece essere localizzato, riceverete il messaggio *Request timed out*.

Potete anche testare se l'accesso ad Internet sia funzionante digitando un indirizzo esterno, ad esempio *www.yahoo.com* (216.115.108.243). Se non conoscete l'indirizzo IP di un sito, potete usare il comando *nslookup*.

nslookup

Con questo comando potete determinare l'indirizzo IP associato ad un sito Internet. Specificate il nome e il comando nslookup restituirà l'indirizzo IP associato.

Sui computer con sistema operativo Windows, potete eseguire questo comando cliccando su *Start*, quindi su *Run*. Digitate quindi un comando come questo:

Nslookup

Cliccate su *OK*.

La finestra *Command Prompt* verrà visualizzata, quindi digitate il nome dell'indirizzo Internet, ad esempio *www.microsoft.com*.

Verrà mostrato l'indirizzo IP associato come segue:

```
Command Prompt - nslookup

Non-authoritative answer:
Name:    www.microsoft.akadns.net
Addresses:  207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases:  www.microsoft.com

> _
```

Per uscire dalla utility nslookup, digitate **exit** e premete **[Enter]** nella finestra di prompt.